



---

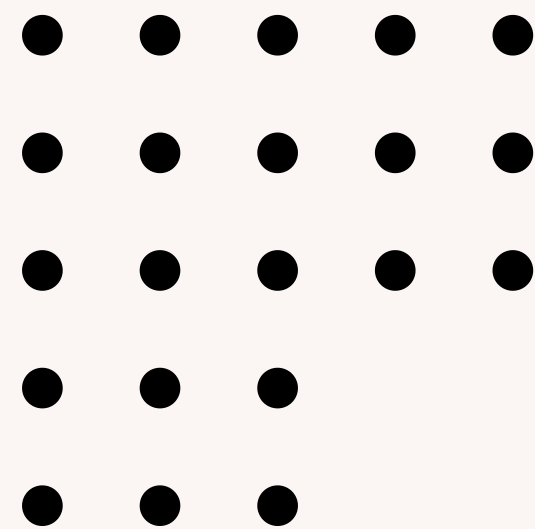
# ANÁLISE DE CÓDIGO COM SONARCLOUD

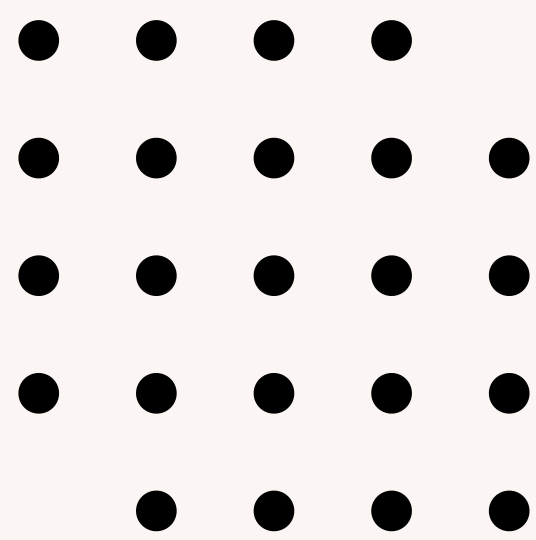
Eduardo de Souza Malagutti - 820649

Enzo Yasumasa Hirotani - 823839

Jonatã Aparecido Reguim - 824754

Vitor Taichi Taira - 823838





# TÓPICOS DE ABORDAGEM

- Referências Utilizadas
- O que é o SonarCloud?
- Principais funcionalidades
- Como começar a usar o SonarCloud

# REFERÊNCIAS UTILIZADAS

- **SonarCloud.** Disponível em: <https://sonarcloud.io>. Acesso em: 10 jun. 2025.
- **SonarCloud: SaaS solution for high quality code.** Disponível em: <https://www.sonarsource.com/products/sonarcloud/>. Acesso em: 10 jun. 2025.
- **SonarQube Cloud Documentation.** Disponível em: <https://docs.sonarsource.com/sonarqube-cloud/>. Acesso em: 10 jun. 2025.
- **Como utilizar o SonarCloud para melhorar a qualidade de código de uma aplicação.** Disponível em: <https://www.ecommercebrasil.com.br/artigos/como-utilizar-o-sonarcloud-para-melhorar-a-qualidade-de-codigo-de-uma-aplicacao>. Acesso em: 10 jun. 2025.



# O QUE É O SONARCLOUD?

A garantia da qualidade de código é essencial para desenvolver software robusto, eficiente e fácil de manter. Ela reduz bugs, melhora a legibilidade, facilita a colaboração em equipe e diminui custos a longo prazo com correções. Práticas como revisões de código, testes automatizados e padronização evitam problemas críticos e garantem entregas mais confiáveis e escaláveis.

O SonarCloud (Atualmente chamada de SonarQube Cloud) da Sonar é uma ferramenta SaaS que auxilia desenvolvedores e organizações a entregar código limpo, integrando-se ao fluxo de trabalho de CI/CD na nuvem



# O QUE É O SONARCLOUD?

Através da metodologia "Clean as You Code" e a funcionalidade "Quality Gates", o código só é liberado para produção se atender aos padrões de qualidade estabelecidos.

Ao se integrar diretamente ao seu pipeline CI ou a uma das plataformas DevOps compatíveis, seu código é verificado contra um extenso conjunto de regras que cobrem diversos atributos do código, como manutenibilidade, confiabilidade e questões de segurança, em cada merge/pull request.



---

# CLEAN AS YOU CODE

- É uma metodologia do SonarCloud que foca na qualidade do código **novo** ou **modificado**, liberando os desenvolvedores da responsabilidade sobre problemas legados. Ela estabelece que cada desenvolvedor é responsável por manter altos padrões no código que escreve no momento, com o SonarQube atribuindo automaticamente a ele os problemas detectados.
-

# EMPRESAS QUE UTILIZAM

CONFIÁVEL PARA MAIS DE 7 MILHÕES DE DESENVOLVEDORES E 400 MIL ORGANIZAÇÕES



Mercedes-Benz



U.S. ARMY



BARCLAYS

AIRFRANCE



CONFIÁVEL PARA MAIS DE 7 MILHÕES DE DESENVOLVEDORES E 400 MIL ORGANIZAÇÕES

Johnson&Johnson



Microsoft



BARCLAYS

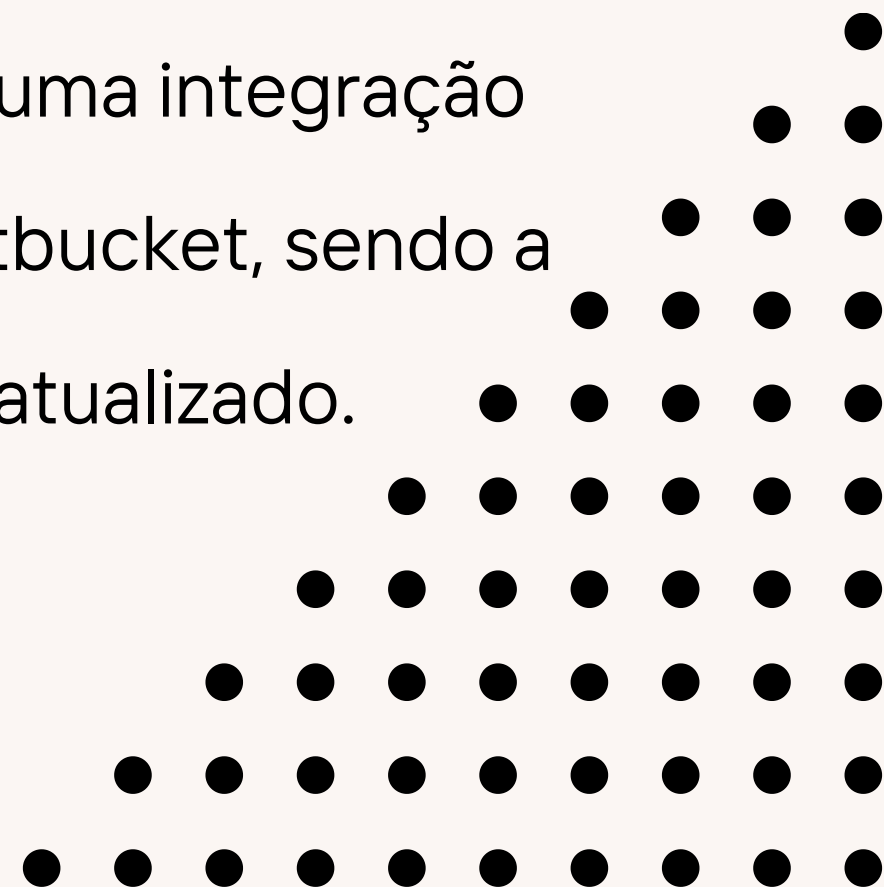
AIRFRANCE



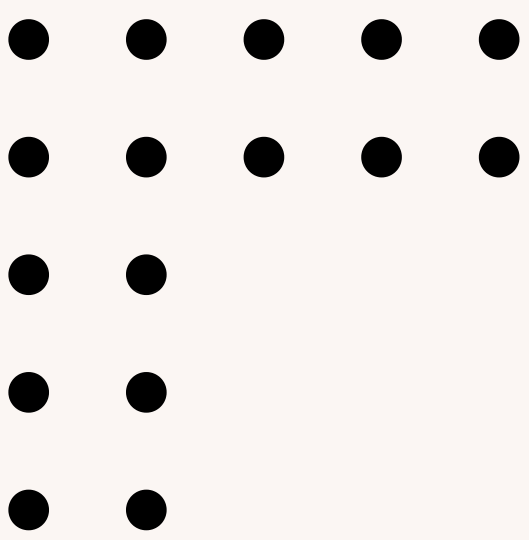


# SONARCLOUD X SONARQUBE

SonarQube é a versão auto-hospedada, exigindo que você instale, gerencie e atualize a plataforma em seus próprios servidores, o que oferece controle total e é ideal para empresas com restrições de dados. O SonarCloud é a versão em nuvem (SaaS) gerenciada pela SonarSource, que elimina a necessidade de manutenção e é otimizada para uma integração contínua e simplificada com repositórios na nuvem como GitHub, GitLab e Bitbucket, sendo a escolha ideal para equipes que buscam agilidade e um serviço sempre atualizado.



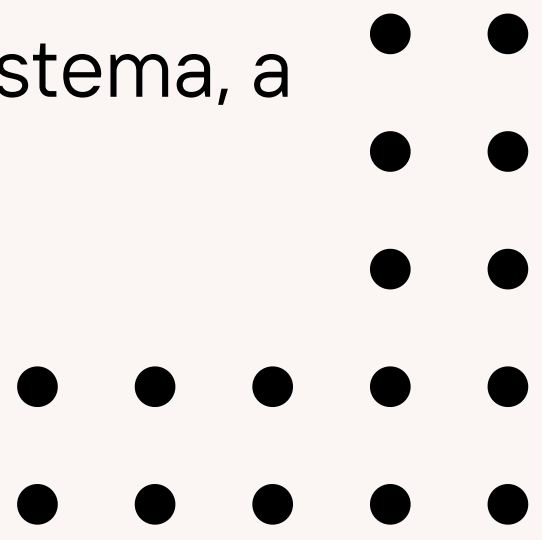




# SONARCLOUD X SONARGRAPH

O **SonarCloud** concentra-se primordialmente na qualidade e segurança do código no nível micro, ou seja, na detecção de bugs, vulnerabilidades, code smells e na aplicação da metodologia "Clean as You Code" e "Quality Gates" para o novo código desenvolvido.

O **SonarGraph** tem seu foco principal na integridade arquitetural e na análise estrutural do software no nível macro. Ele é projetado para arquitetos de software, desenvolvedores sêniores e equipes preocupadas com a manutenibilidade de longo prazo, a complexidade do sistema, a dívida estrutural e a conformidade com as diretrizes arquiteturais definidas



# SONARCLOUD PLANOS

## Livre

Para desenvolvedores que desejam experimentar o SonarQube.

Sempre grátis:

**\$ 0**

Começar

- ✓ Analise seus projetos privados (até 50 mil linhas de código)
- ✓ Escaneie projetos públicos ilimitados
- ✓ 30 linguagens e frameworks ⓘ
- ✓ Máx. 5 usuários
- ✓ Detecção de problemas e SAST
- ✓ Análise de branch principal e pull request
- ✓ Integração da plataforma DevOps

## Equipe

Essencial para equipes e empresas.

Começa em:

~~\$ 65~~ **\$ 32** por mês

Teste gratuito de 14 dias

- ✓ Todos os recursos do nível gratuito mais:
- ✓ Usuários ilimitados
- ✓ Suporte comercial disponível ⓘ
- ✓ SAST avançado
- ✓ Detecção avançada de segredos
- ✓ Código de correção de IA
- ✓ Garantia de código de IA ⓘ
- ✓ Analisar ramificações de recursos e manutenção
- ✓ Personalize os padrões de qualidade

## Empresa

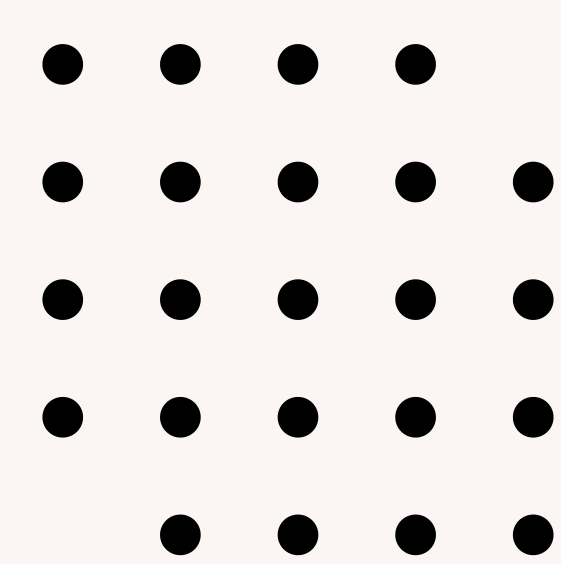
Missão crítica, escalabilidade, desempenho.

Preço anual:

**Falar com vendas**

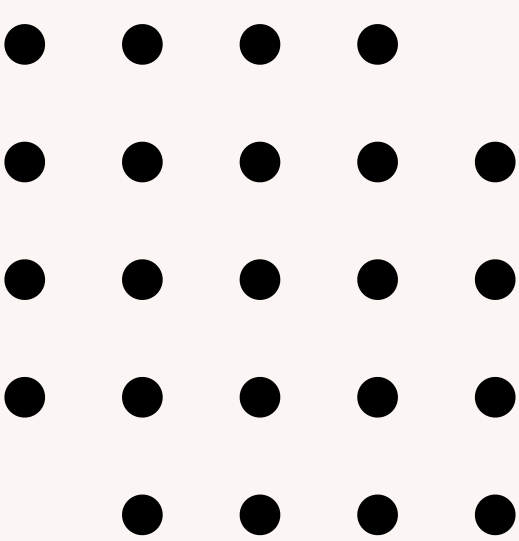
Entre em contato com as vendas

- ✓ Todos os recursos do plano Team mais:
- ✓ 6 idiomas empresariais adicionais ⓘ
- ✓ Suporte comercial disponível ⓘ
- ✓ SLA empresarial
- ✓ Logon único (SSO)
- ✓ Hierarquia da organização empresarial
- ✓ Gestão de portfólio
- ✓ Relatórios de segurança abrangentes ⓘ
- ✓ Informações detalhadas sobre saúde
- ✓ Suporte premium 24 horas por dia, 7 dias por semana (taxa adicional)



# PRINCIPAIS FUNCIONALIDADES.

- Quality Gates (Portões de Qualidade)
- Análise Estática Abrangente e Detecção de Problemas
- Integração Contínua (CI/CD) e Feedback em Pull Requests
- Suporte Multilíngue e Análise Automática
- AI Code Assurance e AI CodeFix
- Análise de Cobertura de Testes
- Integração com IDE via SonarQube for IDE



---

# Quality Gates

Conjuntos de condições baseadas em métricas que o código deve atender para ser considerado apto para produção. O SonarCloud permite definir Quality Gates (Plano Teams) que podem falhar o pipeline de CI/CD se a qualidade e a segurança do código não atenderem aos requisitos estabelecidos. Isso impede que problemas sejam mesclados ou implantados, garantindo que apenas código que atenda ao padrão de qualidade definido seja liberado.

---

# Quality Gates

Os quality gates são ligados à regras e métricas

Java, 1 profile	Projects ?	Rules	Updated	Used
<a href="#">Sonar way</a> BUILT-IN	DEFAULT	562	8 days ago	6 hours ago

A partir das regras que o sonarCloud mostra os erros presentes no nosso código

Intentionality	<a href="#">".equals()" should not be used to test the values of "Atomic" classes</a>	Java	Reliability	Bug	multi-threading
Intentionality	<a href="#">"==" and "!=" should not be used when "equals" is overridden</a>	Java	Maintainability	Code Smell	cert ...
Intentionality	<a href="#">"@Autowired" should be used when multiple constructors are provided</a>	Java	Reliability	Maintainability	Code Smell spring
Intentionality	<a href="#">"@Autowired" should only be used on a single constructor</a>	Java	Reliability	Maintainability	Bug spring

# Quality Gates

Os quality gates são ligados à regras e métricas

## Conditions ⓘ

### Conditions on New Code

Conditions on New Code apply to all branches and to Pull Requests.

No new bugs are introduced

Reliability rating is A

No new vulnerabilities are introduced

Security rating is A

New code has limited technical debt

Maintainability rating is A

All new security hotspots are reviewed

Security Hotspots Reviewed is 100%

New code has sufficient test coverage

Coverage is greater than or equal to 80.0% ⓘ

New code has limited duplications

Duplicated Lines (%) is less than or equal to 3.0% ⓘ

Através dos status das  
métricas que o status  
do quality gate vai  
aparecer Passed ou  
Failed



---

# Análise Estática e Detecção de Problemas

O SonarCloud realiza uma inspeção contínua dos projetos, identificando uma vasta gama de problemas. Dentre eles:

- Bugs
  - Vulnerabilidades de Segurança
  - CodeSmells (Más práticas de código)
-

---

# Análise Estática e Detecção de Problemas

## Bugs

Erros potenciais no código que podem levar a comportamentos inesperados ou falhas em tempo de execução.

### ▼ Type

🐛 Bug 0

🔒 Vulnerability 4


😬 Code Smell 37



# Análise Estática e Detecção de Problemas

## Vulnerabilidades de Segurança

Falhas de segurança, como injeção de SQL, cross-site scripting (XSS) e outras fraquezas que podem ser exploradas por atacantes. O motor de Teste de Segurança de Aplicações Estáticas (SAST) da SonarSource detecta essas vulnerabilidades antes mesmo da compilação e teste da aplicação.




The screenshot displays two identical SonarSource SAST findings for the file `src/.../persistence/repositories/jdbc/DatabaseConnection.java`. Each finding is a security issue with the message "Revoke and change this password, as it is compromised." The severity is "Security" (indicated by a red minus icon). The issue is categorized as "Vulnerability" and "Blocker". The effort is "1h effort" and the age is "22 days ago". The issue is currently "Open" and "Not assigned". The issue key is "L16" for the first and "L28" for the second. The "Responsibility" tab is selected, showing "cwe" and a plus icon. A line from the text "Credentials should not be hard-coded" points to the first finding, and a line from the text "java:S6437" points to the second finding.


src/.../persistence/repositories/jdbc/DatabaseConnection.java


☐ Revoke and change this password, as it is compromised. Responsibility

Security  cwe +

☐ Open ☐ Not assigned L16 • 1h effort • 22 days ago •  Vulnerability •  Blocker

☐ Revoke and change this password, as it is compromised. Responsibility

Security  cwe +

☐ Open ☐ Not assigned L28 • 1h effort • 22 days ago •  Vulnerability •  Blocker

Credentials should not  
be hard-coded  
[java:S6437](#)

# Análise Estática e Detecção de Problemas

## Code Smells (Más Práticas de Código)

Problemas no código que, embora não sejam bugs, indicam um design deficiente, dificultam a manutenção e podem levar a problemas futuros.

src/.../java/br/ufscar/pooa/cinema\_api/CustomMain.java

☐ Replace this use of System.out by a logger. Adaptability  
Maintainability bad-practice cert +  
Open Not assigned L22 10min effort 22 days ago Code Smell Major

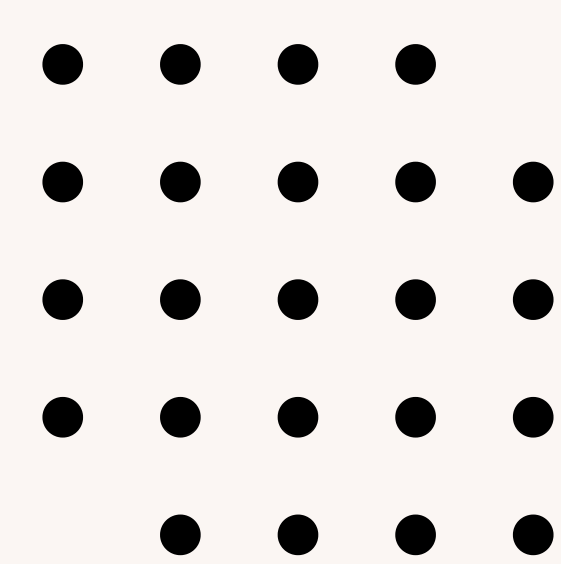
☐ Define and throw a dedicated exception instead of using a generic one. Intentionality  
Maintainability cert cwe ... +  
Open Not assigned L44 20min effort 22 days ago Code Smell Major

---

# Análise Estática e Detecção de Problemas

## Métricas analisadas

- Segurança
  - Reliability (refere-se à capacidade do código de funcionar corretamente sem gerar falhas ou comportamentos inesperados)
  - Manutenibilidade
  - Coverage (mede a porcentagem de linhas que são executadas quando você roda sua suíte de testes.)
  - Duplications
  - Complexidade
-

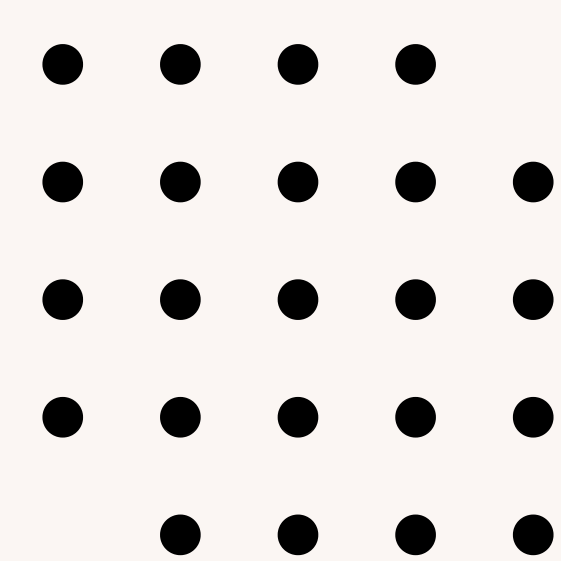


# O QUE O SONARCLOUD PODE FAZER?

## Integração Contínua e Feedback em Pull Requests

- Feedback instantâneo sobre (PRs) ou (MRs), analisando apenas o código novo ou alterado.
- Essa integração permite que a análise de código seja automatizada como parte do pipeline de CI/CD.





---

# O QUE O SONARCLOUD PODE FAZER?

**Suporte Multilíngue e Análise Automática**





# O QUE O SONARCLOUD PODE FAZER?

## AI Code Assurance e AI CodeFix



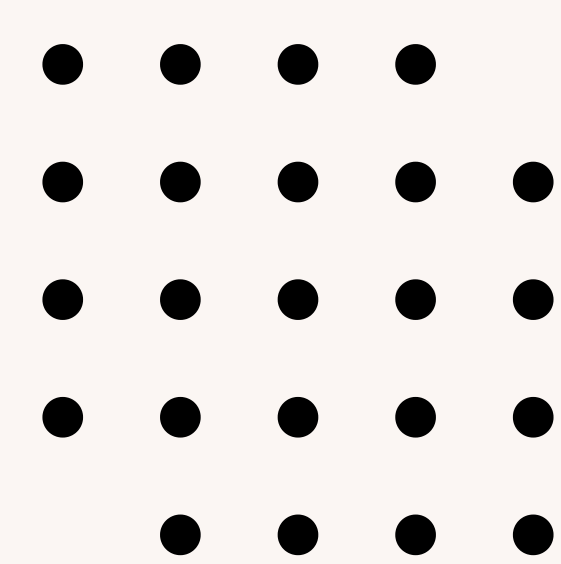
### AI Code Assurance

Sonar AI Code Assurance is a verification process for detecting AI-generated code and then running it through a structured and comprehensive analysis. This ensures all new code meets the highest standards of quality and security before moving to production.



### AI CodeFix

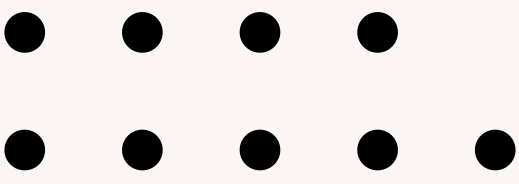
Sonar AI CodeFix leverages LLMs to suggest code fixes for issues detected by SonarQube Server and SonarQube Cloud. With a single click, get AI-driven fix suggestions directly in your IDE on how to resolve a range of issues, streamlining issue resolution.



# O QUE O SONARCLOUD PODE FAZER?

## Análise de Cobertura de Testes

- O SonarCloud avalia a porcentagem de código exercitada por testes, fornecendo insights valiosos sobre a saúde do código. Ele identifica áreas com baixa cobertura de testes que requerem melhorias, ajudando as equipes a focar seus esforços de teste onde são mais necessários.



Spike +

Overview

Boards

Repos

Pipelines

Pipelines

Environments

Releases

Library

Task groups

Deployment groups

Build Tags

Test Plans

Artifacts

Project settings <<

✓ #20240104.9 • LOG-11196 Add Unit Tests Results to Sonar

layoutboards

Run new

This run is being retained as one of 3 recent runs by pipeline.

View retention leases

SummaryTestsExtensionsCode Coverage

Summary

SponsorStar

Information

Parser: Cobertura

Assemblies: 1

Classes: 5

Files: 5

Coverage date: 1/4/2024 - 3:51:30 PM

Line coverage

8%

Covered lines: 19

Uncovered lines: 195

Coverable lines: 214

Total lines: 340

Line coverage: 8.8%

Branch coverage

23%

Covered branches: 12

Total branches: 52

Branch coverage: 23%

Method coverage

Feature is only available for sponsors

Upgrade to PRO version

Risk Hotspots

No risk hotspots found.

Coverage


	Line coverage						Branch coverage			
Name	Covered	Uncovered	Coverable	Total	Percentage		Covered	Total	Percentage	
layoutboards	19	195	214	340	8.8%	<div></div>	12	52	23%	<div></div>
layoutboards.BoardEqulizer	0	46	46	67	0%	<div></div>	0	14	0%	<div></div>
layoutboards.Input	0	51	51	81	0%	<div></div>	0	8	0%	<div></div>
layoutboards.Measurements	0	87	87	128	0%	<div></div>	0	14	0%	<div></div>
layoutboards.Program	0	1	1	1	0%	<div></div>	0	0		<div></div>








# O QUE O SONARCLOUD PODE FAZER?

## Integração com IDE via SonarQube for IDE



**SonarQube for IDE**  
SonarSource  [sonarsource.com](https://sonarsource.com) |  3,546,033 installs |  (117) | Free

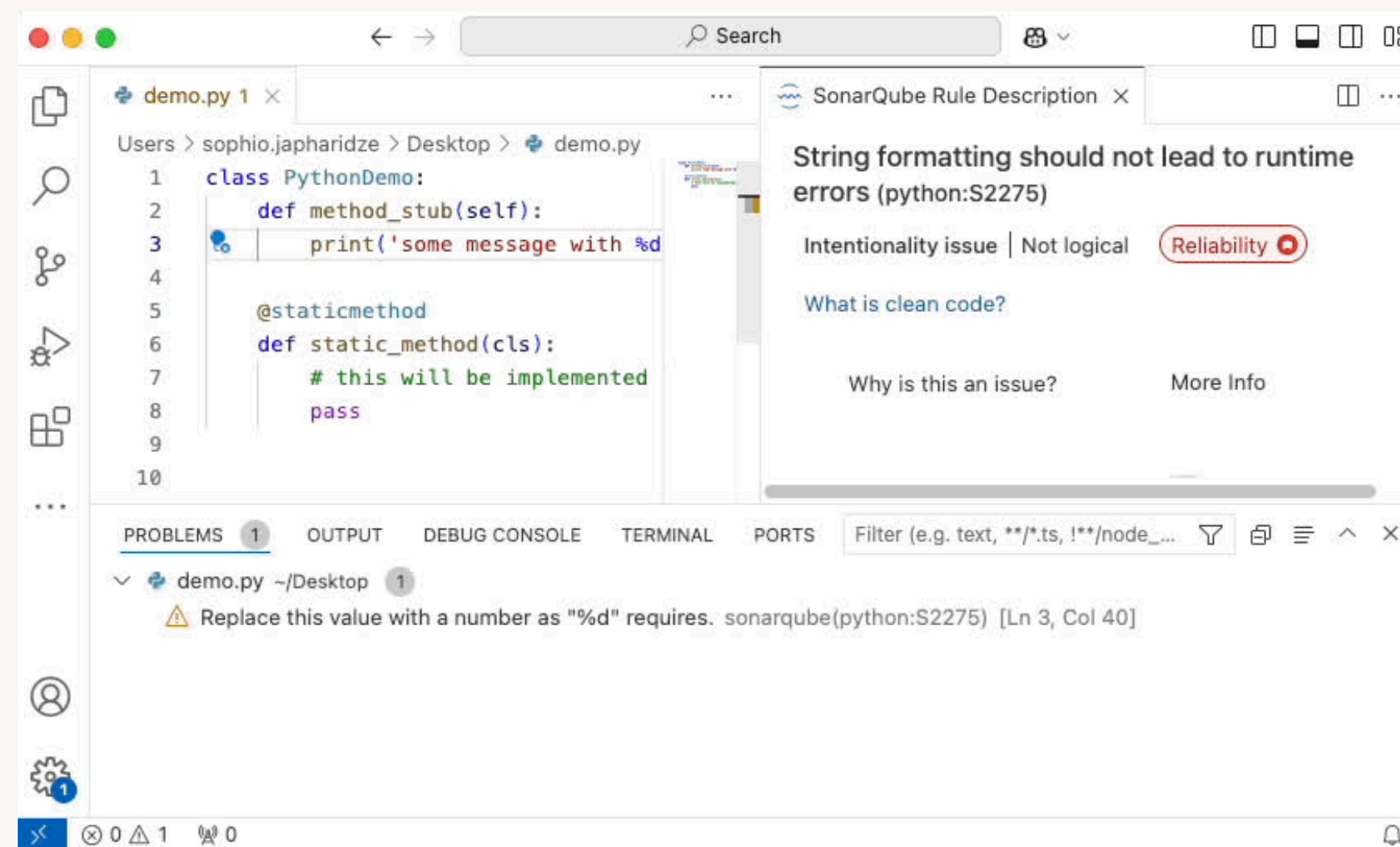
Advanced linter to detect & fix coding issues locally in JS/TS, Python, Java, C#, C/C++, Go, PHP.  
Use with SonarQube (Server, Cloud) for optimal team performance.

[Install](#) [Trouble Installing?](#)

[Overview](#) [Version History](#) [Q & A](#) [Rating & Review](#)

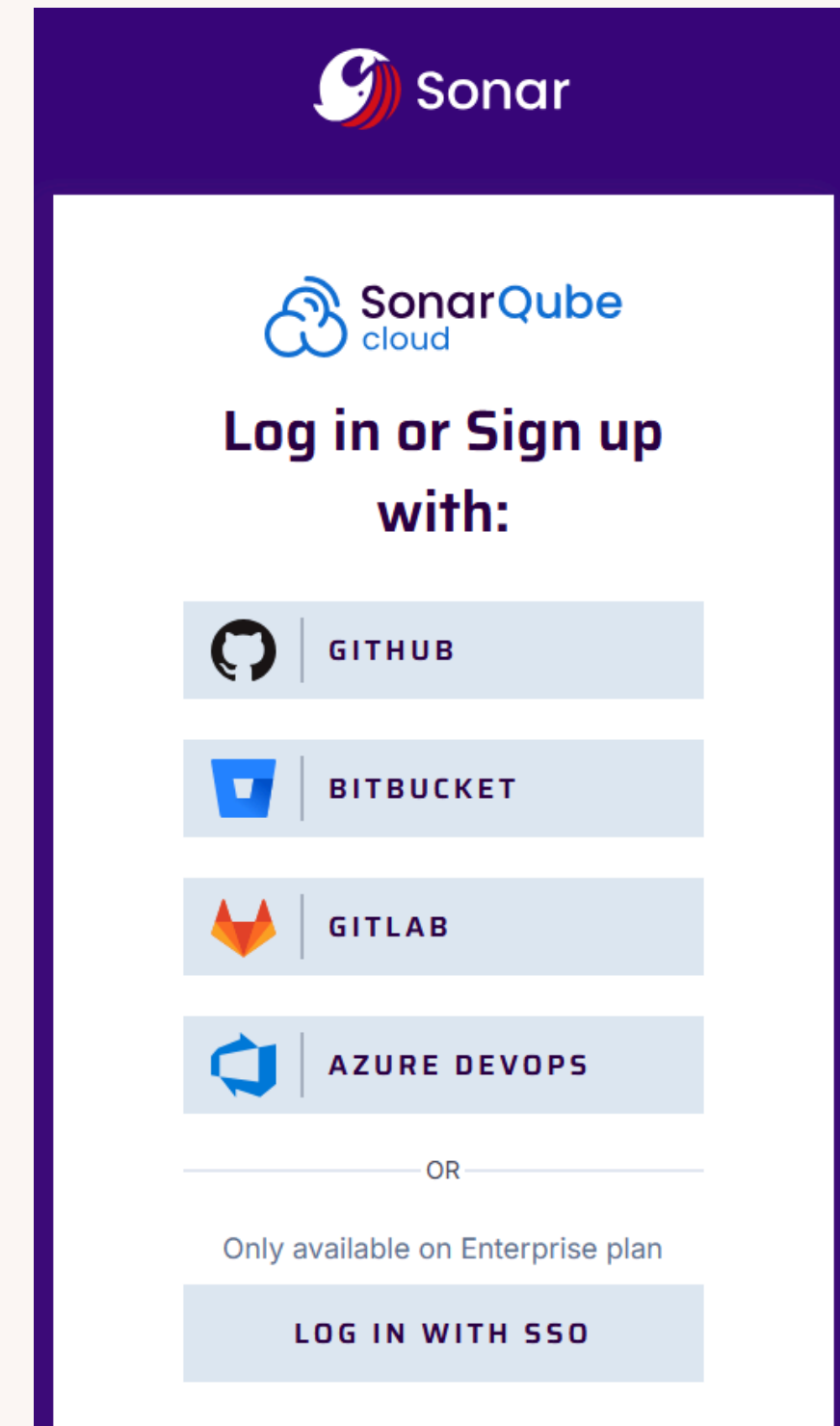
# O QUE O SONARCLOUD PODE FAZER?

Integração com IDE via SonarQube for IDE



# COMO COMEÇAR A USAR?

Se o seu código estiver no GitHub,  
acesse a página do produto  
SonarQube Cloud e escolha Inscrever-  
se (para novos usuários) ou Entrar  
(para usuários existentes) pelo GitHub



Depois de fazer login com sucesso, você verá a tela de boas-vindas do SonarQube Cloud.

Selecione Analyze your first projects > Import an organization from GitHub.

# Welcome to SonarQube Cloud

Let us help you get started in your journey to code quality

## Analyze your first projects

Import projects from a GitHub organization that already have the SonarCloud app installed

 ClaudiaSonarova1 Import >

Or install the SonarCloud app on another of your GitHub organizations

 Import another organization from GitHub

Just testing? You can [create projects manually](#)

## Join an organization

Now that you have an account on SonarCloud, just ask the Organization Administrator to add you manually.


[Learn More](#) 

# CRIE SUA ORGANIZAÇÃO

## Create an organization

Organizations enable your team to collaborate across many projects.

### 1 Import organization details

Import  Enzo Hirotani into a SonarQube Cloud organization ×

Name \*

Up to 255 characters

Key \* ?

Use only lowercase letters, numbers, or hyphens. Must start and end with a letter or number. Up to 255 characters.

[> Add additional info](#)

# ESCOLHA OS REPOSITÓRIOS QUE QUER ANALISAR

## Analyze projects

Select repositories from one of your GitHub organization.


Organization

Enzo Hirotani



Import another organization

☐ Select all available repositories


☐  A-Fuga-das-Galinhas

# DEFINA O QUE SERÁ CONSIDERADO “NEW CODE”

## Set up project for Clean as You Code

The new code definition sets which part of your code will be considered new code.

This helps you focus attention on the most recent changes to your project, enabling you to follow the Clean as You Code methodology.

Learn more: [New Code Definition](#) 

**Set a new code definition for your organisation to use it by default for all new projects**



This can help you use the Clean as You Code methodology consistently across projects.

[Enzo Hirotani - Administration - New Code](#)

The new code for this project will be based on:

☐ **Previous version**

Any code that has changed since the previous version is considered new code.

Recommended for projects following regular versions or releases.

☐ **Number of days**

Any code that has changed in the last x days is considered new code. If no action is taken on a new issue after x days, this issue will become part of the overall code.

Recommended for projects following continuous delivery.




# APRESENTAÇÃO PRÁTICA

[SONARCLOUD.IO](https://sonarcloud.io)






# LISTA DE PROJETOS

 Eduardo Malagutti / POOA-cinema-api

New

Public

 Passed

Last analysis: 10/06/2025, 17:21 · 2.1k Lines of Code · Java, XML, ...

E

4

Security

A

0

Reliability

A


37

Maintainability

E

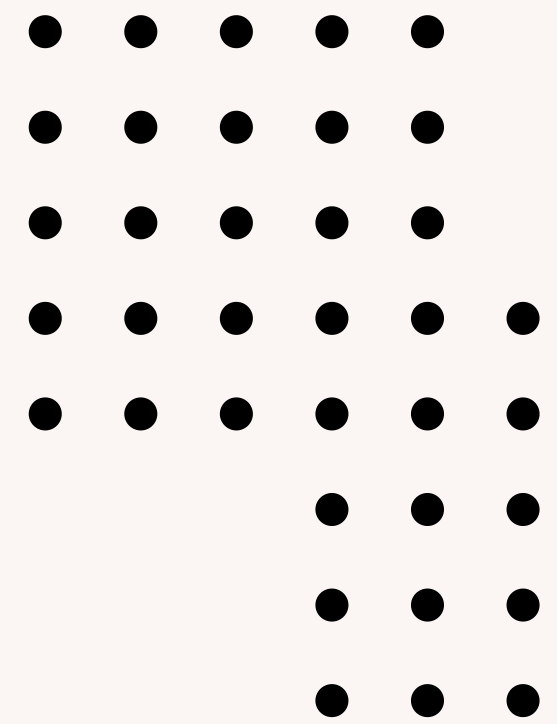
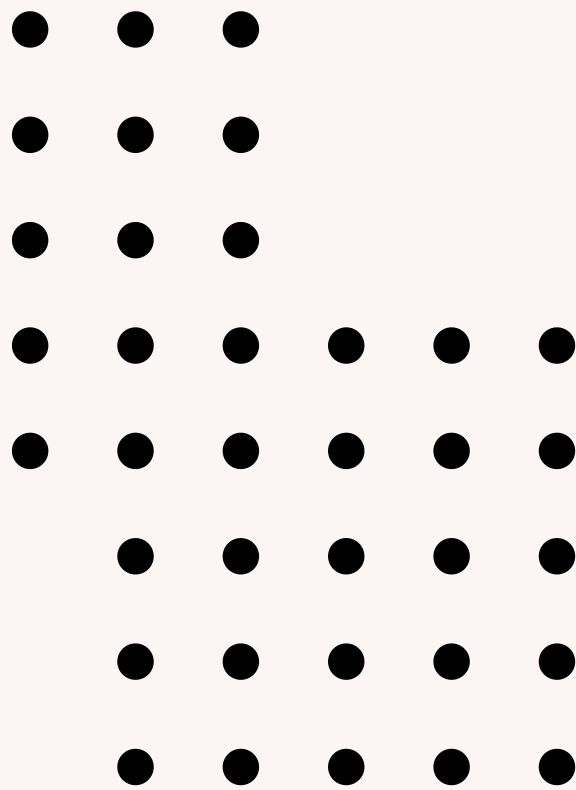
0.0%

Hotspots Reviewed

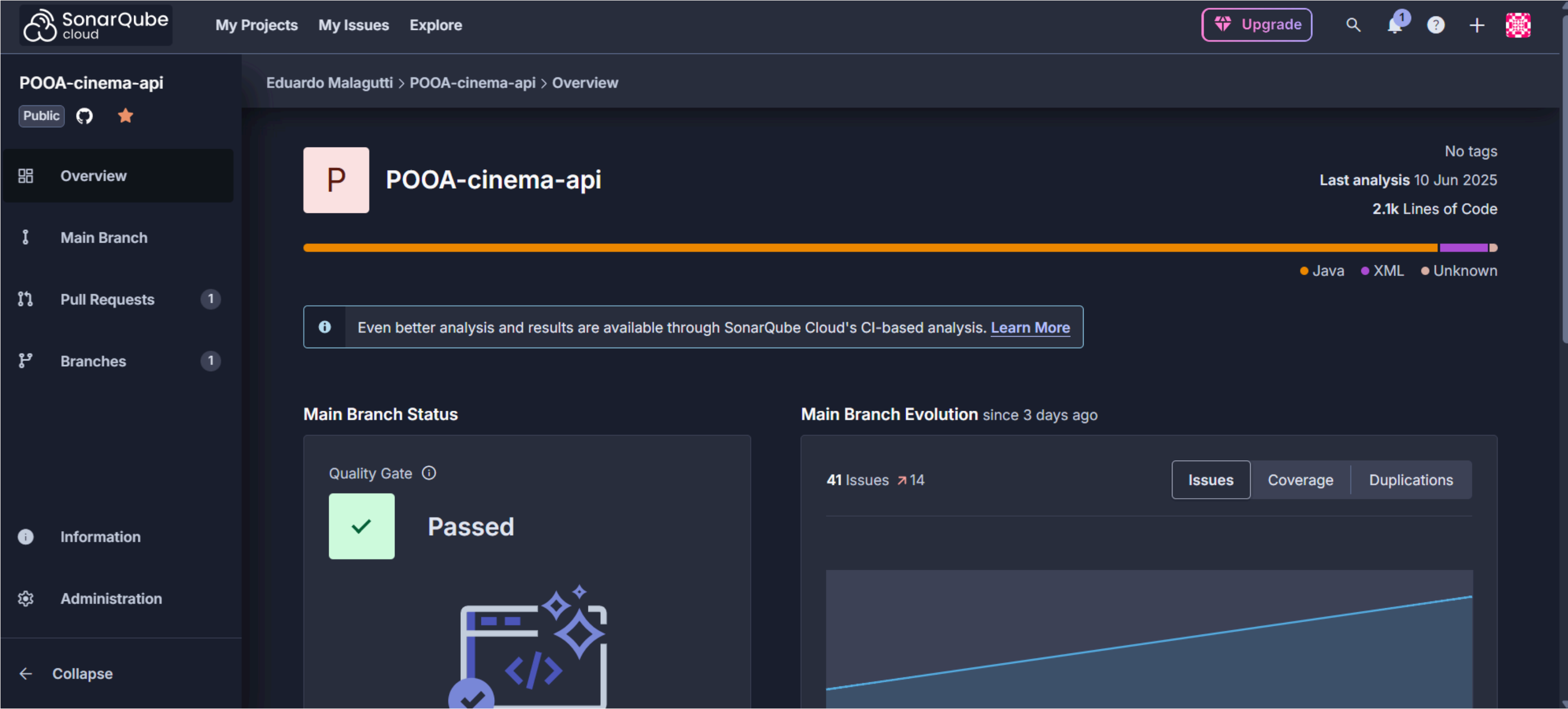


6.5%

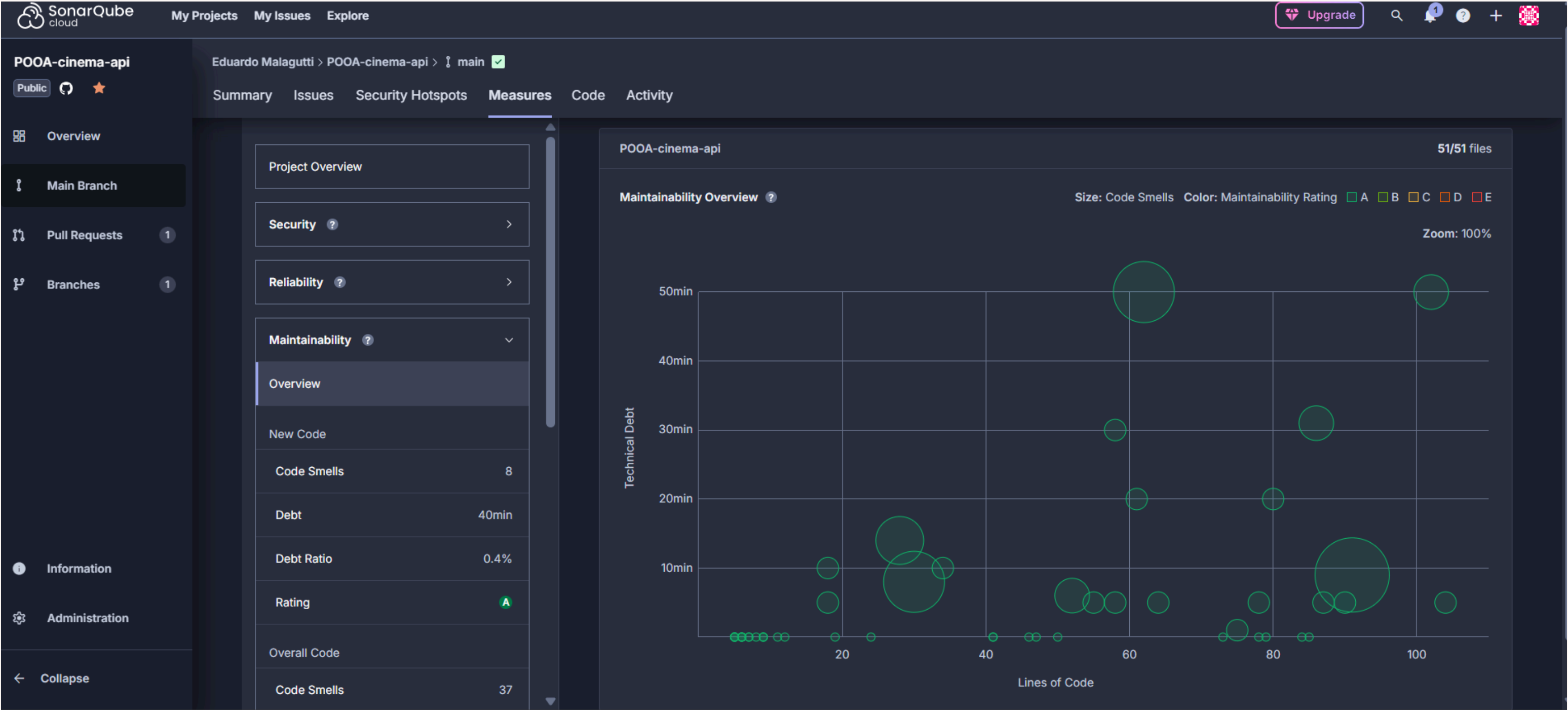
Duplications



# OVERVIEW DE UM PROJETO



# ANÁLISE DE MÉTRICAS DE UMA BRANCH



# ANÁLISE DE PULL REQUESTS

My ProjectsMy IssuesExplore

Upgrade

Search

Notifications

Help

More

Profile

POOA-cinema-api

Public Bind project

Overview

Main Branch

Pull Requests1

Branches1

Information

Administration

Collapse

Eduardo Malagutti > POOA-cinema-api > Pull Requests > 4 – Feat/new db entities

SummaryIssuesSecurity HotspotsMeasuresCode

PR Summary

1k New Lines • Last analysis 3 hours ago • 60e934b5

Quality Gate: Sonar way

Failed

1 condition failed

8.57% Duplicated Lines (%)  
≤ 3.0% required

New Issues

18

No conditions set

Coverage

A few extra steps are needed for SonarQube Cloud to analyze your code coverage.  
[Set up coverage analysis](#)

Accepted Issues

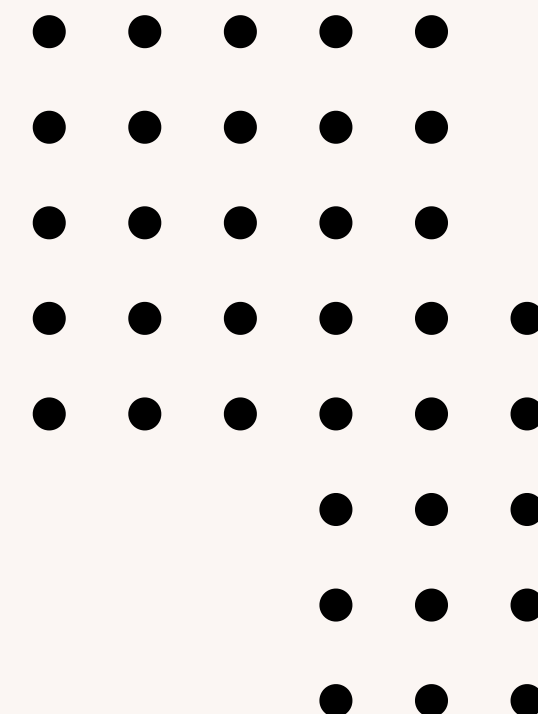
0

Valid issues that were not fixed

Duplications

8.6%

Required ≤ 3.0%  
on 1k New Lines  
6.5% Estimated after merge



**DÚVIDAS?**

