

GIẢI PHÁP SONAR CLOUD CHO PHÁT TRIỂN DỰ ÁN

New Ocean Information System



14+

Years
Experience



100+

Employees



500+

Projects



100%

Clients
Satisfaction



Quality
Management
Systems



Information
Security
Management
Systems

Thử Thách Trong Phát Triển

1 Khó Kiểm Soát Chất Lượng Mã Nguồn 🛑

💡 **Thực tế:** Khi không có công cụ tự động phân tích mã, việc đảm bảo **code sạch** sẽ phụ thuộc vào **review thủ công**, vốn dễ bị **bỏ sót lỗi**.

- ❌ Code smell không được phát hiện sớm, gây ra **nợ kỹ thuật**.
- ❌ Lỗi coding convention không nhất quán, gây **khó đọc & bảo trì**.

📊 Hậu quả:

- ▼ Chất lượng mã kém -> **Tăng thời gian fix bug**.
- ▼ Đội ngũ phát triển mất nhiều thời gian vào **code review thủ công**.

2 Rủi Ro Bảo Mật Cao 🛡️

💡 **Thực tế:** Khi không có **công cụ quét bảo mật**, các lỗ hổng dễ bị bỏ sót.

- ❌ Dễ vi phạm các tiêu chuẩn bảo mật như **OWASP Top 10, PCI DSS**.
- ❌ Không có **Security Hotspots** để kiểm tra lỗ hổng **trong các đoạn code nhạy cảm**.

📊 Hậu quả:

- ▼ Lỗ hổng bảo mật có thể bị khai thác, gây **mất dữ liệu & thiệt hại tài chính**.
- ▼ **Chi phí sửa lỗi bảo mật** sẽ cao hơn nếu phát hiện muộn.

3 Khó Theo Dõi & Kiểm Soát Technical Debt 📉

💡 **Thực tế:** Khi không có SonarCloud, không có cách nào đo lường **technical debt**.

- ❌ Không biết phần nào của codebase cần **tối ưu**.
- ❌ Không có báo cáo về **số lượng code smells, bugs, vulnerabilities**.

📊 Hậu quả:

- ▼ Dự án ngày càng khó bảo trì.
- ▼ Đội ngũ dev phải dành **nhiều thời gian sửa lỗi** thay vì phát triển tính năng mới.

4 Ảnh Hưởng Đến Chất Lượng CI/CD 🚦

💡 **Thực tế:** SonarCloud giúp kiểm tra code trong **quá trình CI/CD**. Nếu không có nó:

- ❌ **Không có Quality Gate** -> Code kém chất lượng có thể bị merge.
- ❌ Không có cảnh báo tự động khi **code có lỗi nghiêm trọng**.

📊 Hậu quả:

- ▼ Tốn công sức để **debug & rollback** khi lỗi xuất hiện trên production.
- ▼ **Tăng thời gian phát triển & release** do phải sửa lỗi muộn.

5 Không Có Báo Cáo & Số Liệu Định Lượng 📊

💡 **Thực tế:** SonarCloud cung cấp **dashboard trực quan** để theo dõi chất lượng mã.

- ❌ Nếu không có SonarCloud, nhóm phát triển **không có dữ liệu đo lường chất lượng code**.
- ❌ Không thể đưa ra quyết định dựa trên số liệu về **bugs, code smells, vulnerabilities**.

📊 Hậu quả:

- ▼ Khó đánh giá mức độ **cải thiện hoặc suy giảm** chất lượng code.
- ▼ Không có số liệu để báo cáo cho **quản lý hoặc khách hàng**.

★ Backend-Fresh-Z NEW PRIVATE

— Not computed

Last analysis: 24/02/2025, 14:44 • 33k Lines of Code • C#, XML, ...

E 16	E 75	A 553	E 0.0%	0.0%	4.3%
Security	Reliability	Maintainability	Hotspots Reviewed	Coverage	Duplications

Sonar Cloud vs DevSecOps

1 SonarCloud Là Gì?

◆ SonarCloud là một dịch vụ phân tích mã nguồn trên nền tảng đám mây giúp các nhóm phát triển cải thiện chất lượng code, giảm nợ kỹ thuật và tăng cường bảo mật.

🚀 SonarCloud được phát triển bởi SonarSource và hỗ trợ hơn 30 ngôn ngữ lập trình như Java, JavaScript, Python, C#, C++, TypeScript,...

💡 SonarCloud tích hợp chặt chẽ với các nền tảng DevOps:

- ✓ GitHub
- ✓ GitLab
- ✓ Bitbucket
- ✓ Azure DevOps

📌 Lợi Ích Chính:

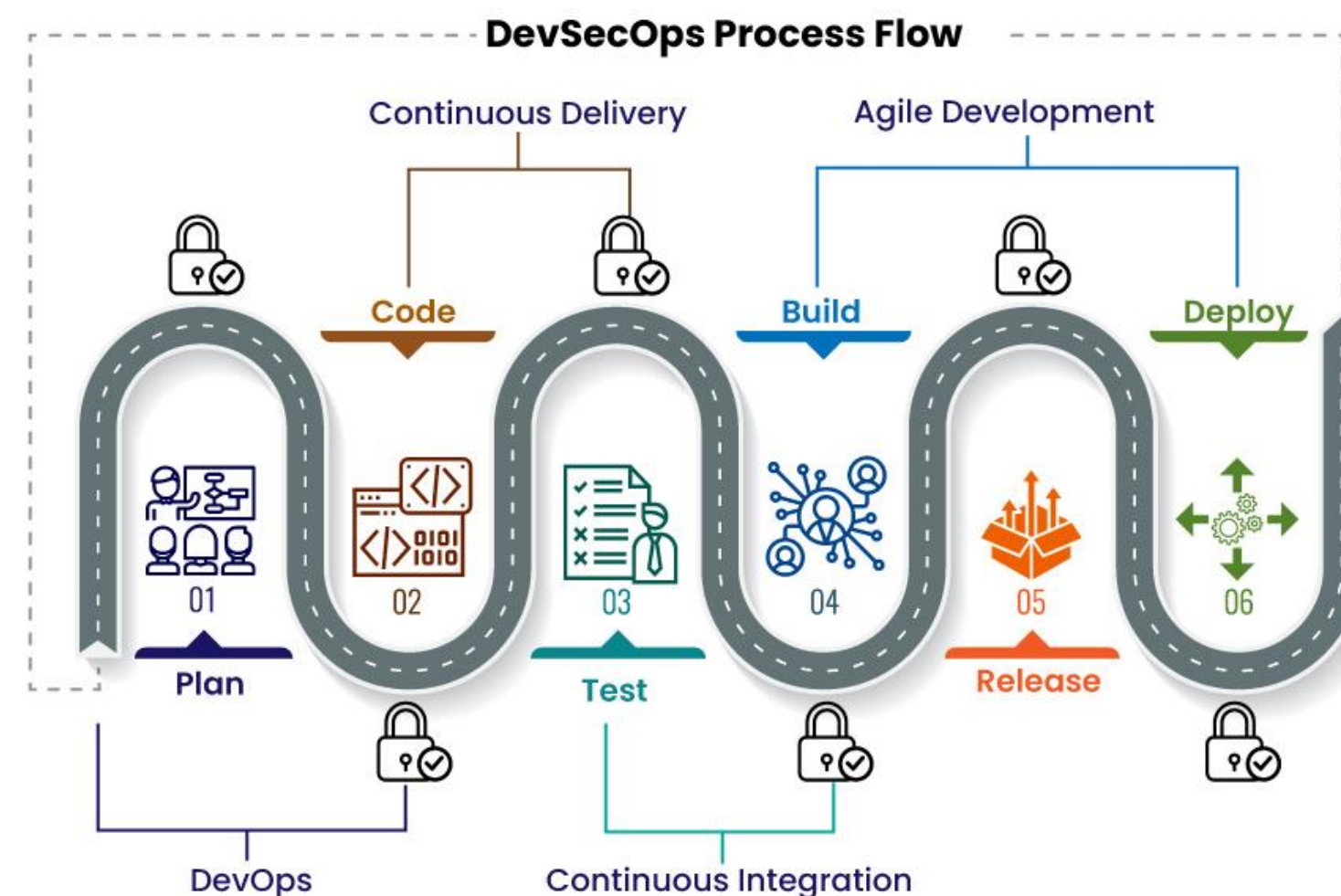
- ✓ Phát hiện & khắc phục lỗi sớm trong quy trình phát triển
- ✓ Tự động quét code trong CI/CD pipeline
- ✓ Cải thiện bảo mật, giảm thiểu rủi ro tấn công
- ✓ Tăng tốc phát triển nhờ code sạch & dễ bảo trì

2 DevSecOps là gì?

DevSecOps (Development + Security + Operations) là một mô hình phát triển phần mềm tích hợp bảo mật vào quy trình DevOps, đảm bảo rằng bảo mật không phải là bước cuối cùng, mà được triển khai xuyên suốt vòng đời phát triển.

📌 Mục tiêu chính của DevSecOps:

- ✓ Phát hiện & sửa lỗi bảo mật sớm trong SDLC
- ✓ Tự động hóa kiểm tra bảo mật trong CI/CD
- ✓ Giảm thiểu rủi ro bảo mật mà không làm chậm phát triển



Chức Năng Cốt Lõi Của SonarCloud

1. Static Code Analysis (Phân Tích Mã Tĩnh)

 SonarCloud **quét mã nguồn tự động** để tìm các vấn đề như:

- ✓ **Bug** 🐛 - Lỗi logic & cú pháp có thể gây lỗi ứng dụng.
- ✓ **Vulnerability** 🛡️ - Lỗ hổng bảo mật có thể bị khai thác.
- ✓ **Code Smell** 🤔 - Mã xấu, khó bảo trì & không tối ưu.

 Ví dụ:

 Nếu một biến được khai báo nhưng không sử dụng, SonarCloud sẽ cảnh báo:

```
let unusedVar; // 🛑 Cảnh báo: Biến này không được sử dụng!
```

3. Quality Gate (Cổng Chất Lượng)

 **Quality Gate** giúp kiểm tra chất lượng code trước khi merge vào nhánh chính.

✓ Thiết lập tiêu chí kiểm tra code như:

- ✓ **Coverage $\geq 80\%$** 🛡️
- ✓ **Không có bug hoặc vulnerability nghiêm trọng** 🚫
- ✓ **Technical Debt phải thấp** 📉

 Nếu không đạt yêu cầu, PR sẽ bị chặn trước khi merge!

 Ví dụ:

 Nếu code coverage $< 80\%$, SonarCloud sẽ không cho merge PR!

5. Technical Debt Management (Quản Lý Nợ Kỹ Thuật)

 SonarCloud **đánh giá mức độ nợ kỹ thuật** trong codebase.

- ✓ **Hiển thị số giờ/công sức cần để sửa code xấu.**
- ✓ **Ưu tiên sửa chữa các vấn đề ảnh hưởng lớn nhất đến hệ thống.**

 **Mục tiêu: Giảm technical debt theo thời gian để code dễ bảo trì hơn.**

2. Security Analysis (Phân Tích Bảo Mật)

 SonarCloud giúp phát hiện các **lỗ hổng bảo mật** theo tiêu chuẩn **OWASP Top 10 & SANS CWE**.

- ✓ **SQL Injection**
- ✓ **XSS (Cross-Site Scripting)**
- ✓ **Hardcoded Credentials**
- ✓ **Command Injection**

 Ví dụ:

 Nếu code chứa thông tin nhạy cảm hardcoded, SonarCloud sẽ cảnh báo:

```
db_password = "123456" # 🛑 Cảnh báo: Không nên hardcode mật khẩu!
```

4. Branch & Pull Request Analysis (Phân Tích Nhánh & PR)

 SonarCloud hỗ trợ **quét code trên từng branch** để đảm bảo code mới không làm giảm chất lượng.

- ✓ **Quét từng Pull Request trước khi merge.**
- ✓ **So sánh chất lượng code giữa các branch.**

 Ví dụ:

 PR chứa lỗi bảo mật => SonarCloud sẽ cảnh báo & chặn merge!

6. CI/CD Integration (Tích Hợp Vào CI/CD)

 SonarCloud dễ dàng tích hợp với Jenkins, GitHub Actions, GitLab CI/CD, Azure DevOps...

- ✓ **Tự động quét code trong pipeline build.**
- ✓ **Không cần cài đặt server, tất cả chạy trên cloud.**

 Ví dụ:

 **Tích hợp SonarCloud với GitHub Actions để kiểm tra code trước khi deploy:**

Quy Trình Hoạt Động Của SonarCloud

📌 Bước 1: Quét Mã Nguồn 🔍

SonarCloud **quét mã nguồn** của dự án thông qua **SonarScanner** để tìm kiếm:

- ✅ **Bug** 🐛 → Lỗi logic, cú pháp sai
- ✅ **Vulnerability** 🛡️ → Lỗ hổng bảo mật (SQL Injection, XSS, Hardcoded Passwords...)
- ✅ **Code Smell** 🗨️ → Mã xấu, khó bảo trì
- ✅ **Coverage** 📊 → Độ phủ của Unit Test

👉 **SonarScanner** có thể chạy trên:

- ✅ **Local** (qua CLI)
- ✅ **CI/CD Pipeline** (GitHub Actions, GitLab CI/CD, Jenkins, Azure DevOps...)

📌 Bước 2: Phân Tích Dữ Liệu 🧠

Sau khi quét mã, SonarCloud **phân tích dữ liệu** dựa trên hơn **6.000 quy tắc kiểm tra** theo các chuẩn:

- 💠 **OWASP Top 10** (Bảo mật Web)
- 💠 **SANS CWE** (Lỗ hổng phần mềm phổ biến)
- 💠 **Code Quality Best Practices** (Quy tắc viết code sạch)

📊 SonarCloud **đánh giá mức độ nghiêm trọng** của vấn đề theo **5 cấp độ**:

🚦 Mức Độ	🔥 Loại Lỗi
🔴 Blocker	Ảnh hưởng nghiêm trọng đến hệ thống
🟠 Critical	Gây lỗi bảo mật hoặc crash hệ thống
🟡 Major	Code khó bảo trì, hiệu suất thấp
🟢 Minor	Không ảnh hưởng lớn nhưng cần cải thiện
🟩 Info	Chỉ là cảnh báo nhẹ

📌 Bước 3: Hiển Thị Báo Cáo Trên Dashboard 📊

Sau khi phân tích xong, SonarCloud **hiển thị báo cáo chi tiết** về lỗi, bảo mật, **technical debt** trên Dashboard.

📌 **Các chỉ số quan trọng:**

- ✅ **Bugs & Vulnerabilities** → Lỗi cần sửa gấp 🔥
- ✅ **Code Smells** → Độ phức tạp & maintainability 🗨️
- ✅ **Test Coverage** → Độ phủ code của Unit Test 🎯
- ✅ **Technical Debt** → Thời gian cần để cải thiện code ⌚

💡 Mọi lỗi sẽ xuất hiện trực tiếp trên **GitHub/GitLab/Jenkins!** 🚀


📌 Bước 4: Áp Dụng Quality Gate 🚦

🚧 **Quality Gate** giúp **ngăn chặn merge code kém chất lượng** vào nhánh chính. Nếu code không đạt tiêu chuẩn, **Pull Request** sẽ bị chặn ❌.

💠 **Tiêu chí mặc định của Quality Gate:**

- ✅ Không có lỗi **Blocker & Critical** 🚫
- ✅ **Code Coverage** ≥ 80% 🛡️
- ✅ **Technical Debt** < 5% tổng thời gian phát triển ⌚

📌 Ví dụ: PR bị chặn do **Code Coverage** thấp ▼

SonarQube
cloud

My ProjectsMy IssuesExplore

Backend-Fresh-Z

PRIVATE

Overview

Main Branch

Pull Requests0

Branches1

Information

Administration

←

Collapse

Industrial-nois > Backend-Fresh-Z > development

SummaryIssuesSecurity HotspotsMeasuresCodeActivity

The last analysis has a warning. [See details](#)

Main Branch Summary

33k Lines of Code • Version 1.0

Quality Gate: [Sonar way](#)

Not computed

Last analysis 23 hours ago • [c9fe4a82](#)

Next scan will generate a Quality Gate.

Security

16 Open issues

E

Reliability

75 Open issues

E

Maintainability

553 Open issues

A

Accepted Issues

0

Coverage

0.0%

No conditions set on 11k Lines to cover

Duplications

4.3%

No conditions set on 58k Lines

Security Hotspots

37

© 2018-2025 SonarSource SA. All rights reserved.

Terms

Pricing

Privacy

Cookie Policy

Security

Community

Documentation

Contact us

Status

About

Demo: Chỉ số Đo Lường Chất Lượng Mã Nguồn



Backend-Fresh-Z

PRIVATE

Overview

Main Branch

Pull Requests0

Branches1

Information

Administration

Collapse

Industrial-nois > Backend-Fresh-Z > development

SummaryIssuesSecurity HotspotsMeasuresCodeActivity

Project Overview

Security

Overview

Overall Code

Vulnerabilities10

RatingE

Remediation Effort3h 30min

Reliability

Overview

Overall Code

Bugs13

RatingE

Remediation Effort1h 55min

Backend-Fresh-Z

500/825 files

Risk

Size: Lines of CodeColor: Worse of Reliability Rating and Security Rating

Zoom: 100%

Coverage

Technical Debt

© 2018-2025 SonarSource SA. All rights reserved.

TermsPricingPrivacyCookie PolicySecurityCommunityDocumentationContact usStatusAbout

Demo: Thống Kê Theo Mã Nguồn



SonarQubecloud

My ProjectsMy IssuesExplore

Backend-Fresh-Z

PRIVATE

OverviewMain BranchPull Requests0Branches1

InformationAdministration

Collapse

Industrial-nois > Backend-Fresh-Z > development

SummaryIssuesSecurity HotspotsMeasuresCodeActivity

The last analysis has a warning. See details

Search for files...

	Lines of Code	Security	Reliability	Maintainability	Security Hotspots	Coverage	Duplications
Backend-Fresh-Z							
Data/Nois.Models	4,743	0	0	31	0	0.0%	1.7%
Library	5,865	7	8	197	26	0.0%	2.8%
Presentation/Nois.Api	22,196	9	63	294	10	0.0%	5.7%
Shared	574	0	4	31	1	0.0%	0.0%

4 of 4 shown

© 2018-2025 SonarSource SA. All rights reserved.

TermsPricingPrivacyCookie PolicySecurityCommunityDocumentationContact usStatusAbout

Demo: Danh Sách Các Lỗi, Cảnh Báo, Và Các Vấn Đề Khác



SonarQube

cloud

My Projects

My Issues

Explore

Backend-Fresh-Z

PRIVATE

Overview

Main Branch

Pull Requests

0

Branches

1

Information

Administration

Collapse

Industrial-nois > Backend-Fresh-Z > development

Summary

Issues

Security Hotspots

Measures

Code

Activity

632 issues

6d 5h effort

Bulk Change

Select issues

Navigate to issue

Data/Nois.Models/Attributes/LevelInformation.cs

Make this class name end with 'Attribute'.

Consistency

Maintainability

convention

Open

Not assigned

L4

5min effort

23 hours ago

Code Smell

Minor

Data/Nois.Models/Attributes/ProductionPlanDescription.cs

Specify AttributeUsage on 'ProductionPlanDescriptionAttribute' to improve readability, even though it inherits it from its base type.

Consistency

Maintainability

api-design

Open

Not assigned

L5

5min effort

23 hours ago

Code Smell

Major

Data/Nois.Models/Dtos/Forms/FormControlJsonDto.cs

Make this field 'private' and encapsulate it in a 'public' property.

Adaptability

Maintainability

cwe

Open

Not assigned

L48

10min effort

23 hours ago

Code Smell

Minor

Data/Nois.Models/Dtos/Forms/FormJsonDto.cs

Make this field 'private' and encapsulate it in a 'public' property.

Adaptability

Maintainability

cwe

Open

Not assigned

L22

10min effort

23 hours ago

Code Smell

Minor

Filters

Software Quality

Security

16

Reliability

75

Maintainability

553

Severity

Blocker

6

High

45

Medium

399

Low

182

Info

0

Clean Code Attribute

Consistency

174

Intentionality

344

Adaptability

105

Responsibility

9

Type

Status

Demo: Chi tiết Vấn Đề



SonarQube

cloud

My ProjectsMy IssuesExplore

Backend-Fresh-Z

PRIVATE

Overview

Main Branch

Pull Requests0

Branches1

Information

Administration

Collapse

Industrial-nois > Backend-Fresh-Z > development

SummaryIssuesSecurity HotspotsMeasuresCodeActivity

1 / 1 issues

Presentation/.../Users/UserService.cs

Change this code to not construct this LDAP name or filter from user-controlled data.

1 execution flow

TokenController.cs

1 SOURCE a user can craft an HTTP request with malicious content

Show 15 more locations

UserService.cs

17 SINK this invocation is not safe; a malicious value can be used as argument

Navigate locations

1 of 1 shown

Intentionality | Not complete

Change this code to not construct this LDAP name or filter from user-controlled data.

LDAP queries should not be vulnerable to injection attacks

Software qualities impacted: Security

OpenNot assignedVulnerabilityBlocker

Where is the issue?Why is this an issue?How can I fix it?ActivityMore info

Presentation/Nois.Api/Controllers/UserManagement/TokenController.cs

25 ...
26 ...
27 ...
28 ...
29 ...
30 ...
31 ...
32 ...
33 ...
34 ...
35 ...
36 ...
37 ...

Presentation/.../Services/UserManagement/Users/UserService.cs

Tags

cwe

Line affected

L489

Effort

30 min

Introduced

23 hours ago

Open in IDE

```
25 ...      /// </summary>
26 ...      /// <param name="model"></param>
27 ...      /// <returns></returns>
28 ...      [AllowAnonymous]
29 ...      [HttpPost]
30 ...      public async Task<IActionResult> 1 Login([FromBody] LoginRequest model)
31 ...      {
32 ...          var resp = await 2 _userService.Validate(model);
33 ...          return Ok(resp);
34 ...      }
35 ...
36 ...      [AllowAnonymous]
37 ...      [HttpGet(".well-known")]
```

Demo: Các Điểm Bảo Mật Cần Xem Xét



SonarQubecloud

My ProjectsMy IssuesExplore

Backend-Fresh-Z

PRIVATE

Overview

Main Branch

Pull Requests0

Branches1

Information

Administration

Collapse

Industrial-nois > Backend-Fresh-Z > development

SummaryIssuesSecurity HotspotsMeasuresCodeActivity

0.0% Security Hotspots Reviewed

To reviewFixedSafe

37 Security Hotspots to review

Review priority: High

Authentication7

"APIKey" detected here, make sure this is not a hard-coded secret.

"ClientSecret" detected here, make sure this is not a hard-coded secret.

"ClientSecret" detected here, make sure this is not a hard-coded secret.

"ClientSecret" detected here, make sure this is not a hard-coded secret.

"Secret" detected here, make sure this is not a hard-coded secret.

"password" detected here, make sure this is not a hard-coded credential.

The last analysis has a warning. See details

"Secret" detected here, make sure this is not a hard-coded secret.

Hard-coded secrets are security-sensitive csharpstuid:S6418

Status: To Review

This Security Hotspot needs to be reviewed to assess whether the code poses a risk.

Review

Where is the risk?What's the risk?Assess the riskHow can I fix it?Activity

Presentation/Nois.Api/appsettings.json

Show 72 more lines

73"LocalAd": {74" "LdapServer": "192.168.15.107",75" "DistinguishedName": "CN=Users,DC=indus,DC=com"76},77" "CaptchaSettings": {78" "Secret": "6LFG53123shA45FAKEAAAA01m4LkHrrTk0V5buEFOfnsezwnNF",79" "Url": "https://www.google.com/recaptcha/api/siteverify"80}81// "ApiConfigs": {82// "Greeter": {83// "Uri": "https://localhost:5001"

Show 11 more lines

Review priority: High

Category: Authentication

Assignee: Not assigned

© 2018-2025 SonarSource SA. All rights reserved.

TermsPricingPrivacyCookie PolicySecurityCommunityDocumentationContact usStatusAbout

Chi Phí và Báo Giá



Billing & Upgrade

Here you can manage your subscriptions for Industrial-nois.

Current plan

Modify plan

Free

- Up to 50k private lines of code
- Up to 5 members
- Unlimited public lines of code

Members

1 / 5 members

Lines of Code used

33,378 private lines of code analyzed over 3 projects

50k

Billing and payment information

Edit


Use our Customer Portal to:

- View or update your billing and payment information
- View or download your past invoices

	Free <div>Current plan</div>	Team <div>Free trial available</div>	Enterprise
	\$0	Starting at \$64 \$32/month = 50% off	To get started Talk to sales
		<div>Start Free Trial</div>	<div>Contact sales</div>
Members	Up to 5	Unlimited	Unlimited
Private lines of code	Up to 50k	Up to 1.9M	Unlimited
Public lines of code	Unlimited	Unlimited	Unlimited
Highlights			
Feedback on branches	—	✓	✓
Custom Quality Profile and Quality Gate	—	✓	✓
Authentication	DevOps Platform	DevOps Platform	SSO
AI CodeFix	—	✓	✓
Enterprise hierarchy and reporting	—	—	✓
Commercial support	—	—	✓ 5M lines of code and above
Additional packs			
Premium support	—	✓	✓

Kết Luận

SonarCloud là một công cụ quan trọng trong DevSecOps, giúp kiểm tra chất lượng code, phát hiện lỗi bảo mật & tối ưu hóa mã nguồn.

- ✓ Tích hợp vào CI/CD để quét code tự động mỗi lần push hoặc mở PR.
- ✓ Phát hiện lỗi sớm (Bug, Vulnerability, Code Smell) trước khi triển khai.
- ✓ Quality Gate  giúp chặn merge code kém chất lượng.
- ✓ Hỗ trợ bảo mật theo tiêu chuẩn OWASP Top 10, CWE, SANS.
- ✓ Giúp team DevOps & Security tiết kiệm thời gian & tăng tốc phát triển phần mềm.

 Tóm lại: SonarCloud không chỉ là một công cụ quét mã nguồn mà còn là một phần quan trọng của DevSecOps, giúp đảm bảo bảo mật & hiệu suất phần mềm ngay từ giai đoạn phát triển. 

Q&A - Các Câu Hỏi Thường Gặp

? 1. SonarCloud có miễn phí không?

- ✓ Có! SonarCloud miễn phí cho các dự án mã nguồn mở (public projects).
- ✗ Với các dự án private, cần đăng ký gói trả phí theo số Lines of Code (LoC).

? 3. Làm sao để tối ưu Quality Gate trong SonarCloud?

 Mặc định Quality Gate kiểm tra:





- ✓ Code Coverage $\geq 80\%$
- ✓ Không có lỗi Blocker & Critical
- ✓ Technical Debt $< 5\%$ tổng thời gian phát triển

 Bạn có thể tùy chỉnh trong SonarCloud Dashboard! 

? 2. SonarCloud có hỗ trợ tất cả các ngôn ngữ lập trình không?

- ✓ SonarCloud hỗ trợ hơn 30 ngôn ngữ, bao gồm:
- ◆ Java, JavaScript, Python, C, C++, C#, TypeScript, Go, PHP, Kotlin, Swift,...

? 4. Nếu không sử dụng SonarCloud, có rủi ro gì?

- ✗ Không kiểm soát được lỗi bảo mật 
- ✗ Code kém chất lượng, khó bảo trì 
- ✗ CI/CD dễ bị lỗi khi deploy 
- ✗ Dự án dễ mắc nợ kỹ thuật cao 

 SonarCloud giúp phát hiện lỗi sớm, tiết kiệm thời gian & chi phí phát triển phần mềm!



CONTACT US

Microsoft
Partner



Gold Application Integration
Gold Data Analytics
Gold Application Developments
Gold Cloud Platform

 **Microsoft**
Solutions Partner

Data & AI
Azure



BRONZE
System Integrator

A ROCKWELL AUTOMATION PARTNER



DATALOGIC
ISV PARTNER

Get in touch if you would like to discuss how **New Ocean IS** can assist you with your technology journey.

E: info@nois.vn

P: (+84) 28 6681 0782

W: www.nois.vn