

Strengthening Your FOSS Project: Essential Files & Automated License Compliance (FOSSA-CLI)

PRESENTER : SANTHOSH NC | DATE: 26/09/2025

Greetings & Welcome to the session



FOSS Meetup - September

Talk

Strengthening Your FOSS Project: Essential Files And Automated License Compliance (FOSSA-CLI)

27-Sept-2025, Saturday

2PM - 6PM

Dr. Mahalingam College of Engineering
and Technology



Santhosh N C

Lead Infrastructure Consultant,
Thoughtworks



To-Do List

- ▶ About Me
- ▶ A Game
- ▶ **#1 Essential Files**
- ▶ **#2 Automated License Compliance (FOSSA-CLI)**
- ▶ Hands-on Demo (If Possible)
- ▶ Final Words

**When the meeting
has no agenda...**



👋 Hi, I'm Santhosh NC.md

MARKDOWN

```
1 # 👋 Hi, I'm Santhosh NC
2 📁 **Lead Infra Consultant @ ThoughtWorks** | 📅 **9+ Years Experience**
3 ✨ **CNCF Kubestronaut**
4 ---
5 ### 🧑💻 Expertise
6 DevOps • DevSecOps • MLSecOps
7
8 ### 📜 Certifications
9 GCP (13) • Kubernetes (5) • GitHub (5) • AWS (11)
10
11 ### 🎯 Interests
12 Tech Enthusiast • Aspiring Bus Driver • Meme Engineer
13
14 ---
15 > _Always exploring, learning and sharing tech with the community._
16
```

👋 Hi, I'm Santhosh NC

📁 **Lead Infra Consultant @ ThoughtWorks** | 📅 **9+ Years Experience**
🔗 **CNCF Kubestronaut**

🧑💻 Expertise

DevOps • DevSecOps • MLSecOps

📜 Certifications

GCP (13) • Kubernetes (5) • GitHub (5) • AWS (11)

🎯 Interests

Tech Enthusiast • Aspiring Bus Driver • Meme Engineer

Always exploring, learning and sharing tech with the community.

What's the first thing that comes to your mind when you hear **FOSS**?



“

#1 Strengthening Your FOSS Project: Essential Files

”

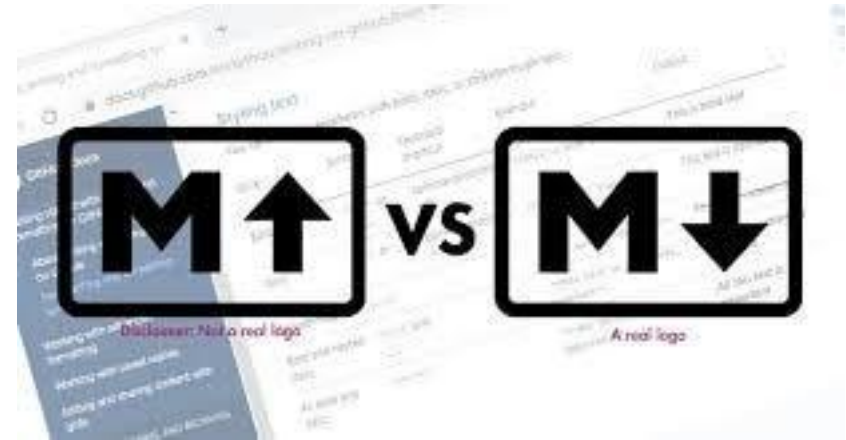
#1 Strengthening Your FOSS Project: Essential Files

- ▶ Reduce friction for newcomers
- ▶ Make maintainers' lives easier
- ▶ Increase trust and adoption
- ▶ Encourage repeat contributions
- ▶ Protect both the community and the maintainers



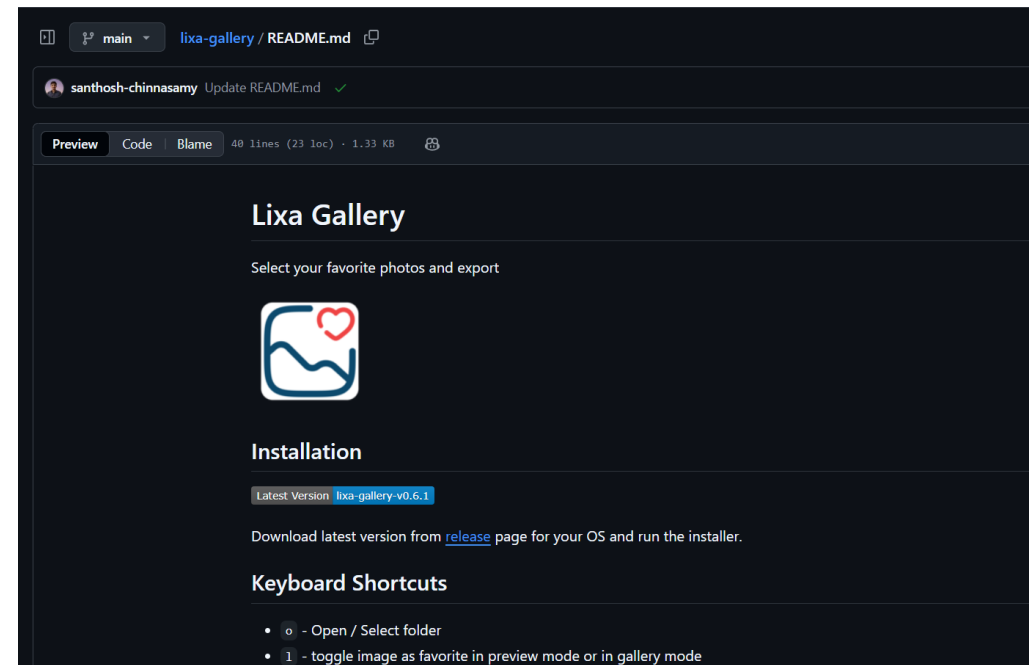
Markup and Markdown language

- ▶ **Markup** is a general term for content formatting - such as HTML
- ▶ But **markdown** is a library that generates HTML markup.



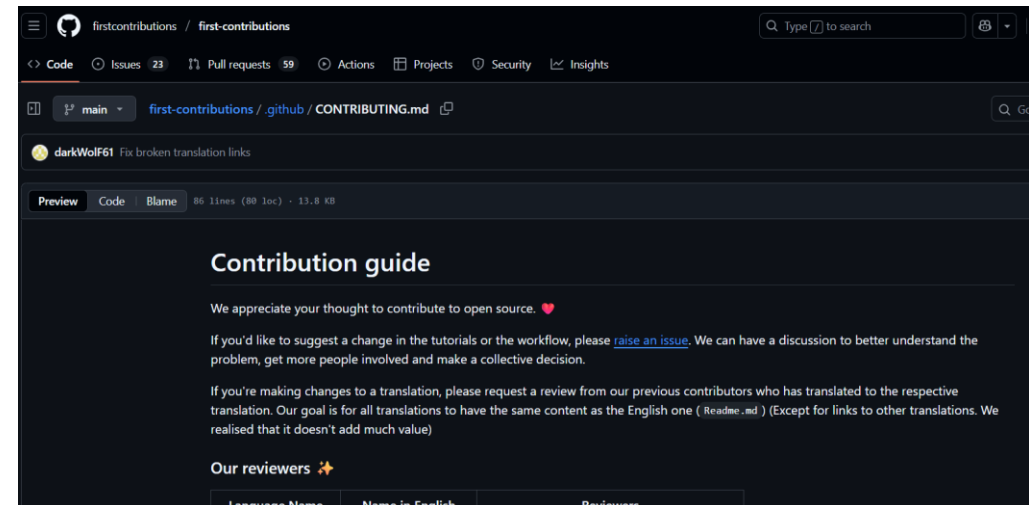
#1 README.md

- ▶ The project's landing page: what it does, how to install, basic usage.
- ▶ **First impressions** – A clear README.md explains what the project does and how to use it.



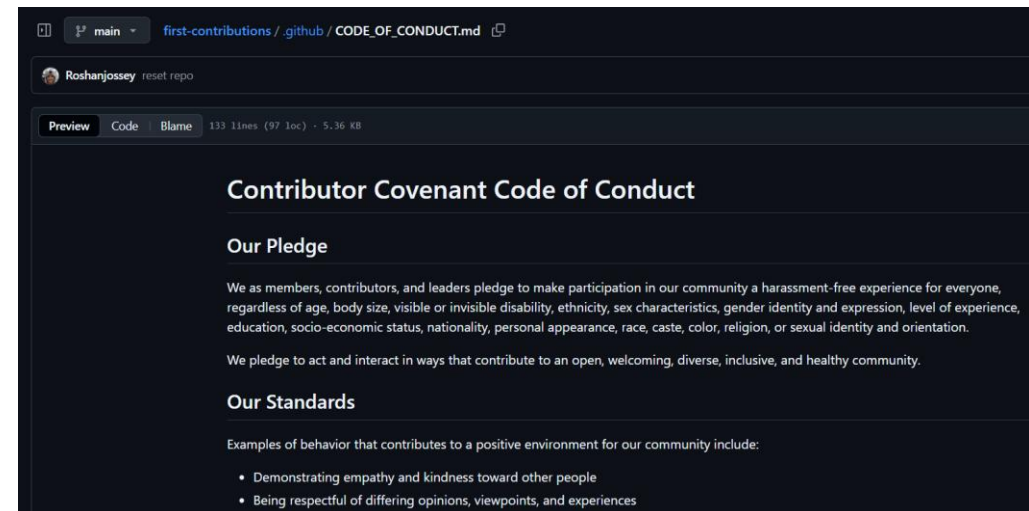
#2 CONTRIBUTING.md

- ▶ How to contribute: coding standards, PR process, branching strategy, issue filing.
- ▶ **Onboarding** – CONTRIBUTING.md gives newcomers step-by-step instructions, reducing questions and bad PRs.



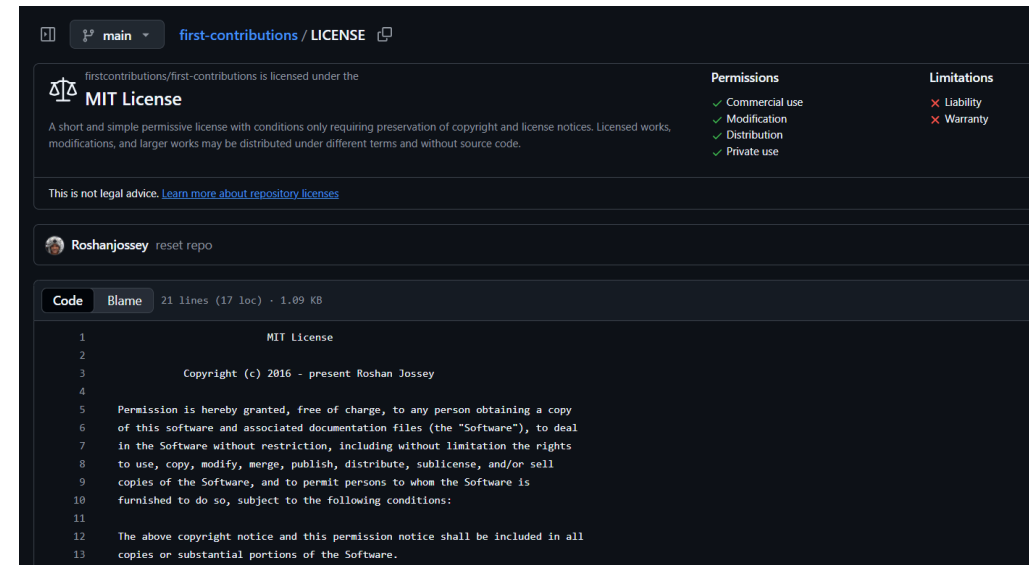
#3 CODE_OF_CONDUCT.md

- ▶ Expected behavior, reporting abusive conduct; helps maintain a healthy community.
- ▶ **Safe environment** – CODE_OF_CONDUCT.md sets behaviour expectations and shows the project welcomes all.



#4 LICENSE

- ▶ Legal terms; tells others how they can use and share the code.
- ▶ **Legal clarity** – LICENSE tells users and contributors how they can use, modify, and distribute the code.

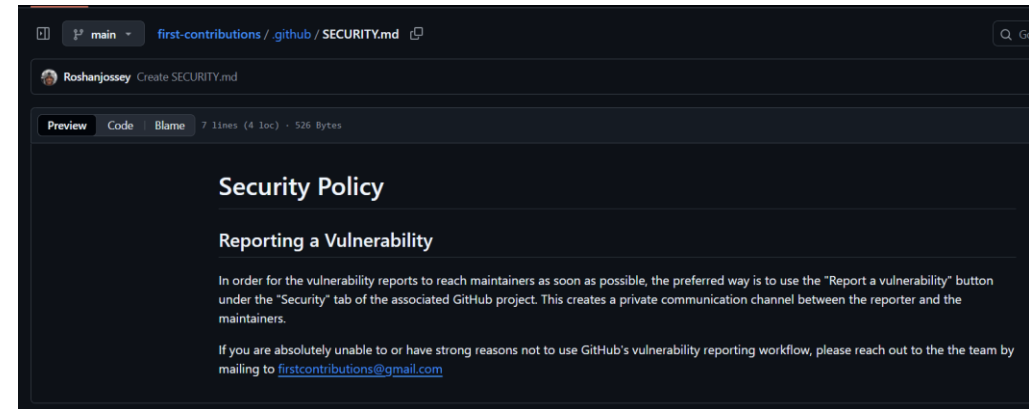


The screenshot shows the GitHub interface for the MIT License. At the top, it says "firstcontributions / LICENSE". Below this, it states "firstcontributions/first-contributions is licensed under the MIT License". A short description follows: "A short and simple permissive license with conditions only requiring preservation of copyright and license notices. Licensed works, modifications, and larger works may be distributed under different terms and without source code." To the right, there are two columns: "Permissions" and "Limitations". The "Permissions" column lists: "Commercial use", "Modification", "Distribution", and "Private use", all with green checkmarks. The "Limitations" column lists: "Liability" and "Warranty", both with red X marks. Below this, there is a note: "This is not legal advice. [Learn more about repository licenses](#)". Further down, the user "Roshanjossey" is shown with a "reset repo" button. At the bottom, the "Code" tab is selected, showing the full text of the MIT License in a code editor format.

```
1      MIT License
2
3      Copyright (c) 2016 - present Roshan Jossey
4
5      Permission is hereby granted, free of charge, to any person obtaining a copy
6      of this software and associated documentation files (the "Software"), to deal
7      in the Software without restriction, including without limitation the rights
8      to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
9      copies of the Software, and to permit persons to whom the Software is
10     furnished to do so, subject to the following conditions:
11
12     The above copyright notice and this permission notice shall be included in all
13     copies or substantial portions of the Software.
```

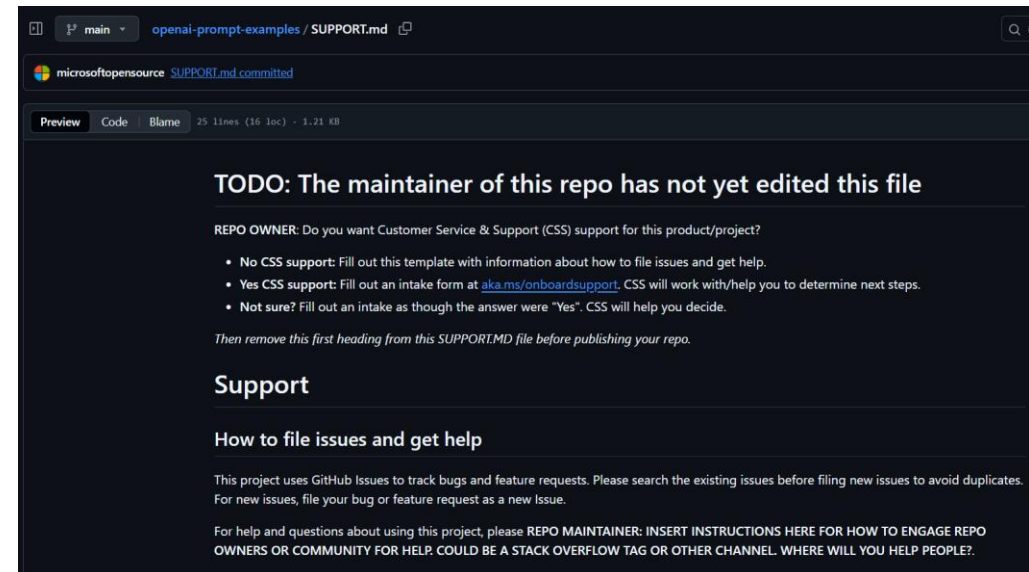
#5 SECURITY.md

- ▶ How to responsibly report vulnerabilities or security issues.
- ▶ **Security** – SECURITY.md gives a private channel for vulnerability reports so they're not posted publicly.



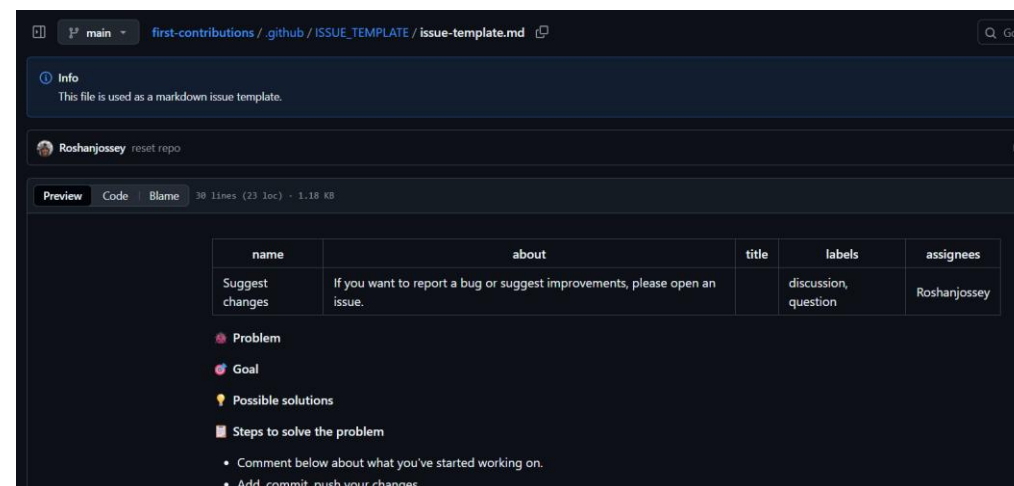
#6 SUPPORT.md

- ▶ Where to ask questions, links to docs, Slack/Discord/Forum.
- ▶ **Support channel** – SUPPORT.md points people to the right forum, Slack, or docs instead of filing issues.



#7 .github/ISSUE_TEMPLATE/*.md

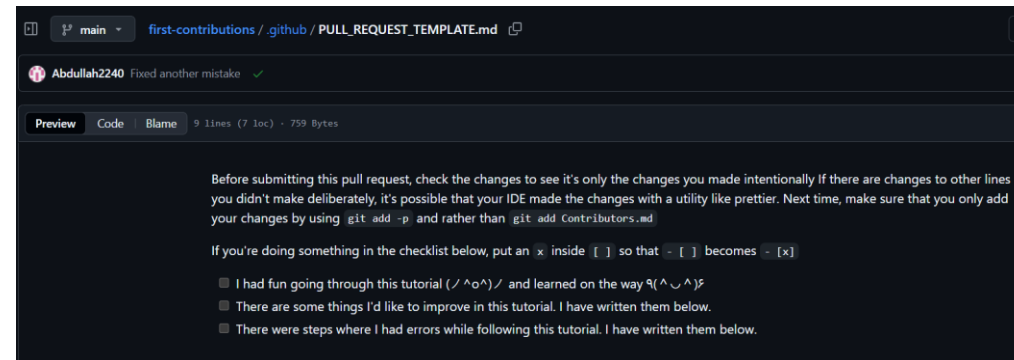
- ▶ Pre-defined templates for bug reports, feature requests.
- ▶ **Predictable templates** – Issue and PR templates help gather the right information and speed up review.



#7

.github/PULL_REQUEST_TEMPLATE.md

- ▶ Pre-filled checklist and guidelines for PRs.
- ▶ **Predictable templates** – Issue and PR templates help gather the right information and speed up review.



#8 FUNDING.yml

- ▶ Tells GitHub where to direct people who want to financially support the project.
- ▶ **Sustainability** – FUNDING.yml provides a clear way for sponsors and supporters to financially back the project, helping maintainers sustain and grow their work.

How do I display Patreon, Open Collective, or another external funding platform on a project?

You can display one or more external funding options by adding them to your **FUNDING.yml** file:

```
patreon:          patreon_username
open_collective:  open_collective_username
ko-fi:            ko-fi_username
tidelift:         tidelift_package_name
community_bridge: community_bridge_username
liberapay:        liberapay_username
issuehunt:        issuehunt_username
otechie:          otechie_username
custom:           ["custom_url.com", "another_custom_url.com"]
```

Path for about default community health files

- ▶ The **.github** folder
- ▶ The **root** of the repository
- ▶ The **docs** folder

Special file - .gitignore

- ▶ Ignoring files
- ▶ You can configure Git to ignore files you don't want to check in to GitHub.
- ▶ This is useful for keeping log files, temporary files, build artifacts, or personal files out of your repository.

“

#2 Automated License Compliance (FOSSA-CLI)

”

fossas / fossa-cli

- ▶ **Zero-configuration polyglot tool** – works with any codebase or build automatically.
- ▶ **Automatic dependency detection** – supports multiple languages and build tools.
- ▶ **Extra scanning features** – limited support for vendored dependencies, containers, and system libraries (WIP).
- ▶ **FOSSA integration** – performs license scanning, vulnerability checks, and generates attribution reports.
- ▶ **Goal** – become a universal tool for dependency analysis.

fossas/fossa-cli

Fast, portable and reliable dependency analysis for any codebase. Supports license & vulnerability scanning for large monoliths. Language-agnostic; integrates with...



58

Contributors

21

Used by

1k






Stars

185

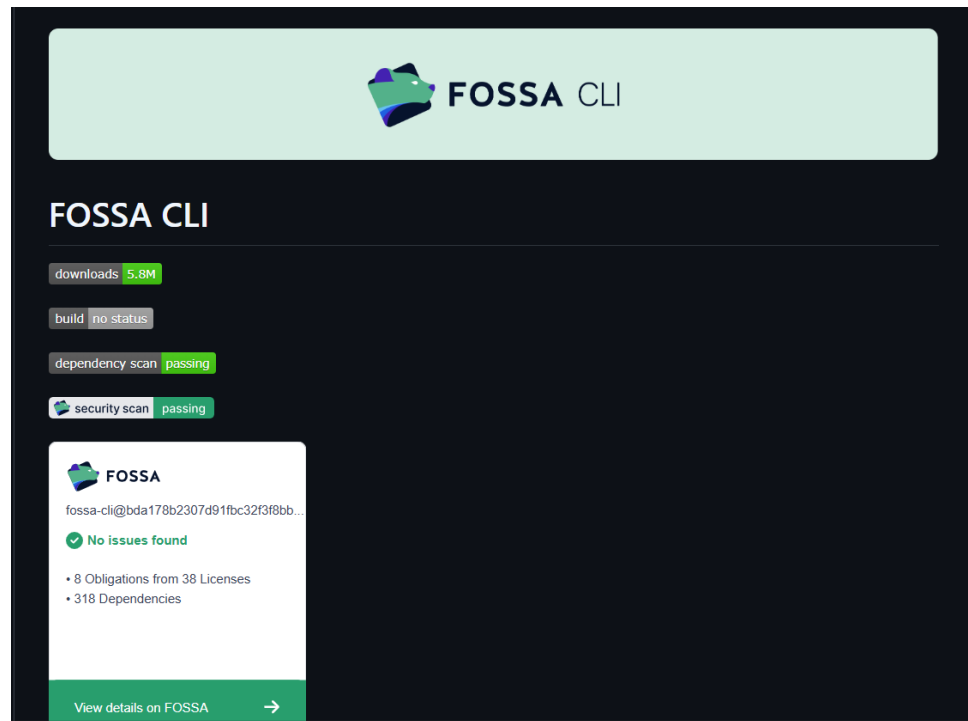
Forks



Analogy / Example

- ▶ Imagine your **open-source project** is like a **college group project**.
 - ▶ Your **codebase** = the project report you and your team are writing.
 - ▶ **Dependencies** = the references, books, or resources you cite in your report.
 - ▶ **Licenses & vulnerabilities** = the rules about using those resources (like plagiarism rules or outdated/mistaken info).
- ▶ **FOSSA CLI** is like a **super vigilant project checker** for your group:
 - ▶  **Checks references** – ensures you're allowed to use them (license compliance).
 - ▶  **Spots risky sources** – prevents potential issues (vulnerability detection).
 - ▶  **Examines references of references** – catches hidden risks (transitive dependencies).
 - ▶  **Integrates with workflow** – continuously reviews new additions (like a vigilant teacher).
 - ▶  **Generates a report card** – shows which references are safe, risky, or need fixes (comprehensive reporting).

fossa-cli example



My contribution to the Open source community

- ▶ Mentees from 7+ Colleges
- ▶ AI / ML Domain
- ▶ With the guidance of an AIML researcher based out of German
- ▶ Collaborating with 140+ Students
- ▶ GitHub
- ▶ GHAS
- ▶ Badges via Badgr



Using
Free and Open
Source
Software (FOSS)

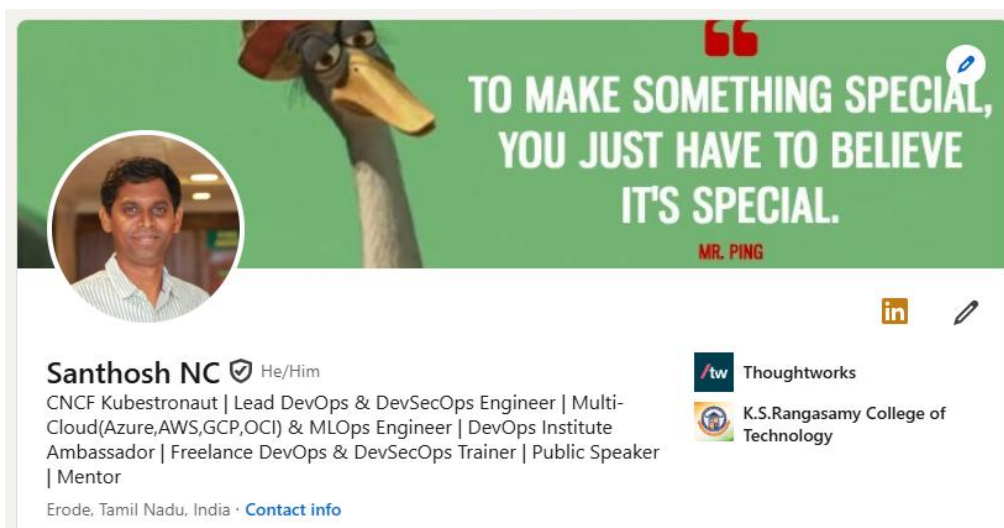
Contributing
to Free and
Open Source
Software (FOSS)

Personal touch meme

WHAT GIVES PEOPLE
FEELINGS OF POWER





Let's Connect



TO MAKE SOMETHING SPECIAL,
YOU JUST HAVE TO BELIEVE
IT'S SPECIAL.

MR. PING

Santhosh NC He/Him
CNCF Kubestronaut | Lead DevOps & DevSecOps Engineer | Multi-Cloud(Azure,AWS,GCP,OCI) & MLOps Engineer | DevOps Institute Ambassador | Freelance DevOps & DevSecOps Trainer | Public Speaker | Mentor
Erode, Tamil Nadu, India · [Contact info](#)

 Thoughtworks
 K.S.Rangasamy College of Technology



“

Thank you

”