



DevOps Meets AI: Automating Reliability in the Age of Intelligence

Speaker: Patrick Bashizi

Event: Build With AI - GDG Kinshasa 2025

Date: 10 May 2025



by Patrick Bashizi



About the Speaker

1 Role

Patrick Bashizi is a Lead Systems Engineer at C Squared.

2 Specialty

He specializes in Cloud, DevOps and Site Reliability Engineering

3 Passion

He is passionate about intelligent automation and AI-driven DevOps innovation.

4 Focus

He focuses on building self-healing systems by combining observability, automation, and AI; while actively contributing to open-source tools.

5 In the Past

Patrick has over 10 years of Software Engineering, all Platforms included.

He is the founder of the GDG Kishasa Community in July 2011



Problem Statement



Modern systems are highly complex, distributed, and fast-changing

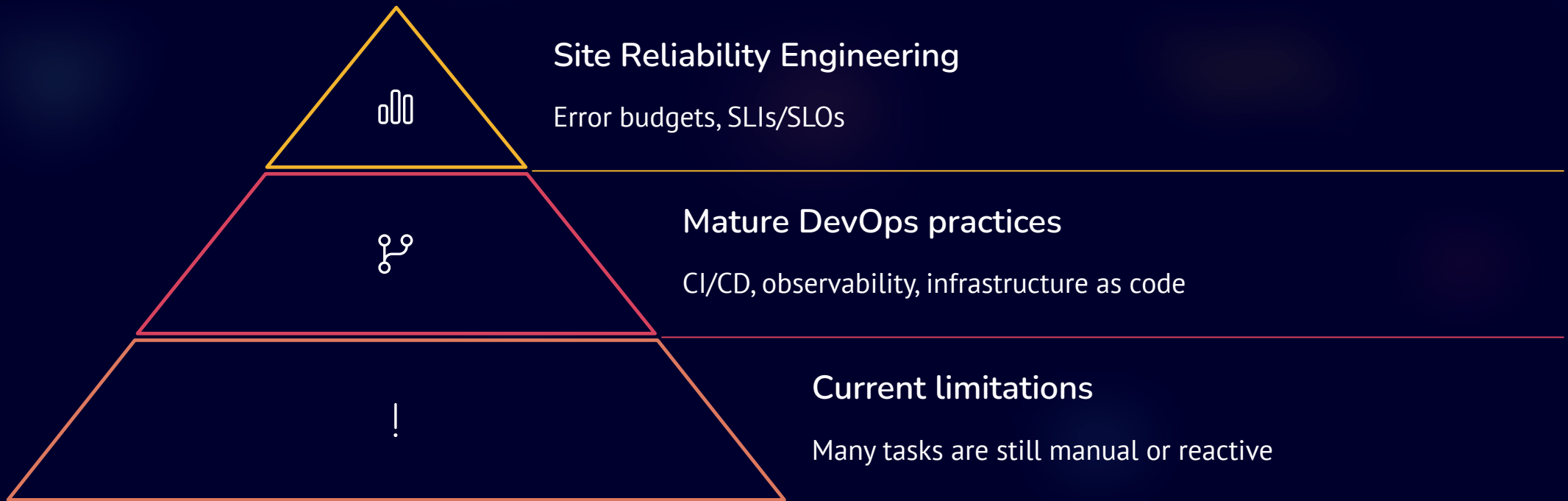


Ensuring reliability is harder than ever



Ops teams are overwhelmed with alerts, incidents, and manual toil

DevOps Today



The AI Shift in DevOps

Manual Operations 🧑

Manual fixes, scripting, and toil dominate this stage.

- High toil and repetitive alerts
- Reactive response to issues

1

AI-Augmented DevOps 🤖

AI empowers self-healing, predictive alerts, and dynamic decisions.

- Intelligent insights leading to action
- Proactive, autonomous operations



2

3

Traditional DevOps 🧑

Focus on automation, CI/CD pipelines, and monitoring.

- Efficiency via dashboards and alerting
- Reactive or partial automation

The AI Shift



Data Collection

AI can learn from logs, metrics, traces, and code patterns



Intelligence Layer

Move from reactive to predictive incident management



Augmentation

Augment DevOps with intelligent automation



Demo Introduction

Objective

Use AI to analyze PRs and suggest fixes in real-time

Live Demo

Let's walk through a live demo of AI-enhanced DevOps

Technology Stack

GitHub, Cloud Build, Trivy, Vertex AI, Cloud Functions

Pipeline Architecture

1 Developer PR

Developer opens or updates a Pull Request on GitHub

4 AI Integration

Python script processes results and provides feedback



2 GitHub Actions

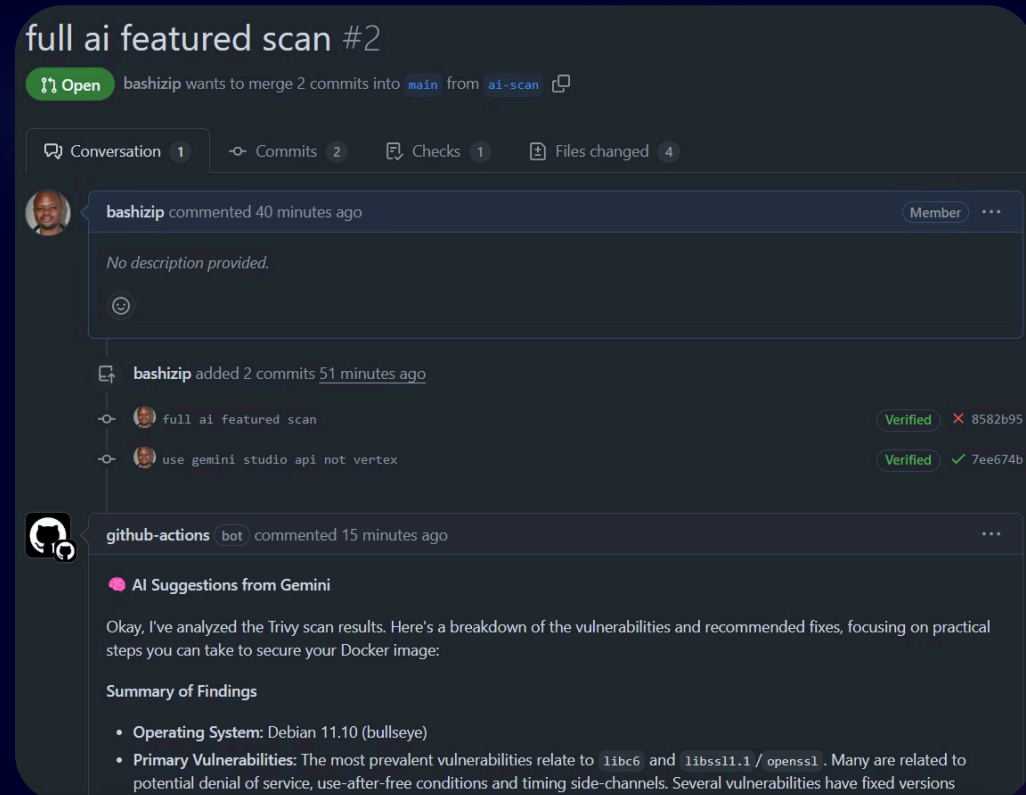
Workflow is triggered automatically

3 CI Pipeline Steps

- Checkout code
- Build Docker image from Dockerfile
- Scan image using Trivy
- Save scan results as JSON

AI in Action

PR Suggestions



The screenshot shows a GitHub pull request titled "full ai featured scan #2". The pull request is open, showing a conversation between a user named "bashizip" and the "github-actions" bot. The "bashizip" comment, posted 40 minutes ago, states "No description provided." and includes a sad face emoji. The "github-actions" bot comment, posted 15 minutes ago, provides "AI Suggestions from Gemini". The bot's message includes a summary of findings from a Trivy scan, highlighting vulnerabilities in the operating system and specific libraries.

full ai featured scan #2

Open bashizip wants to merge 2 commits into `main` from `ai-scan`

Conversation 1 · Commits 2 · Checks 1 · Files changed 4

bashizip commented 40 minutes ago Member

No description provided.

bashizip added 2 commits 51 minutes ago

- full ai featured scan Verified ✗ 8582b95
- use gemini studio api not vertex Verified ✓ 7ee674b

github-actions bot commented 15 minutes ago

AI Suggestions from Gemini

Okay, I've analyzed the Trivy scan results. Here's a breakdown of the vulnerabilities and recommended fixes, focusing on practical steps you can take to secure your Docker image:

Summary of Findings

- Operating System:** Debian 11.10 (bullseye)
- Primary Vulnerabilities:** The most prevalent vulnerabilities relate to `libc6` and `libssl1.1 / openssl`. Many are related to potential denial of service, use-after-free conditions and timing side-channels. Several vulnerabilities have fixed versions

Key Characteristics

- Clarity in explanations
- Accuracy of suggestions
- Developer-friendly tone

Emphasize how AI augments—not replaces—human review

Benefits Observed



Faster pull
request reviews



Early detection of
security issues



Less manual
effort in triage
and remediation



Consistent
feedback across
teams



Challenges & Limits



Trust issues

Trust in AI-generated suggestions?



AI limitations

Handling hallucinations and false positives



Resource concerns

Cost and performance tuning of AI pipelines



Human oversight

Need for human oversight and guardrails



What's Next & Conclusion

Future Developments

- Smart incident routing and auto-resolution
- AI-assisted root cause analysis (RCA)
- Feedback loops to continuously improve suggestions
- Integration with observability and incident tools

Conclusion

DevOps is evolving with AI at its side

Embrace intelligent automation to boost reliability

Collaboration between Devs, Ops, and AI is the future

Thank You! Questions?

Feel free to reach out for more insights and discussion.

1

Blog

Learn more at blog.patrickbashizi.com

2

Contact

Visit patrickbashizi.com for details

3

Connect

Follow me on [X](#), [LinkedIn](#) and [GitHub](#)