

# I Break Things, AI Fixes Them: Building a Self-Healing CI/CD Pipeline

Premved Dhote

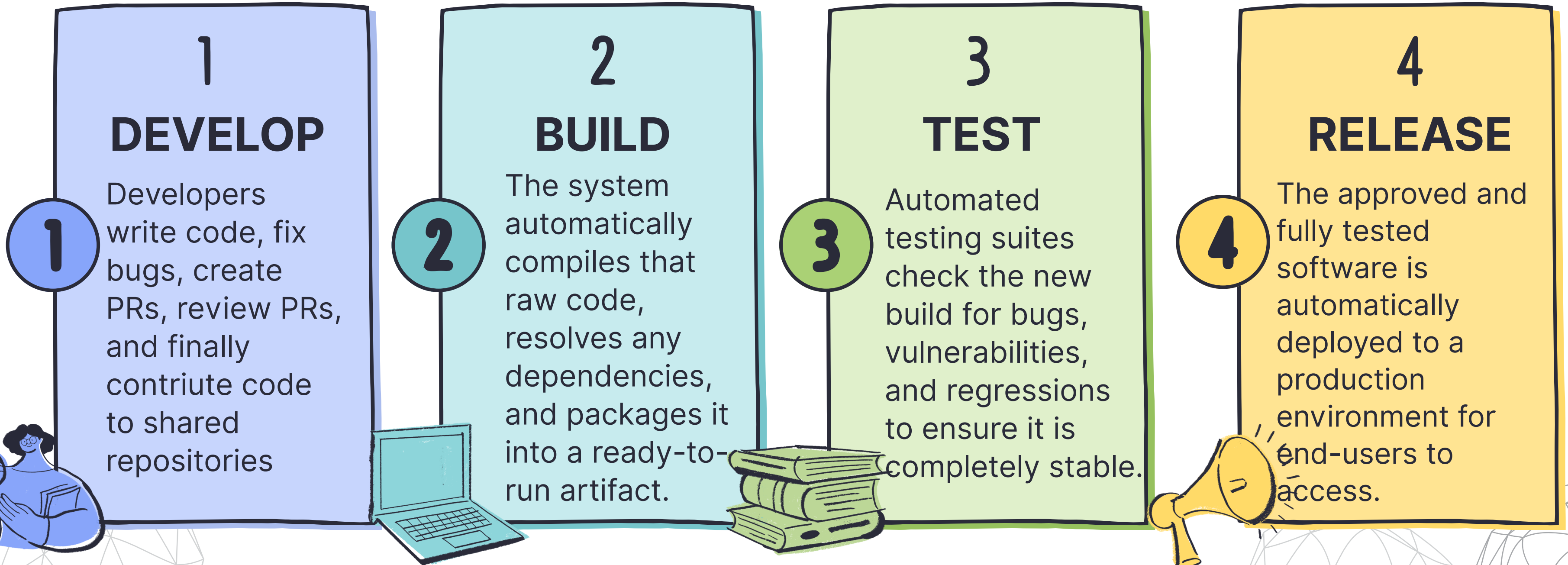
Software

Engineering Intern

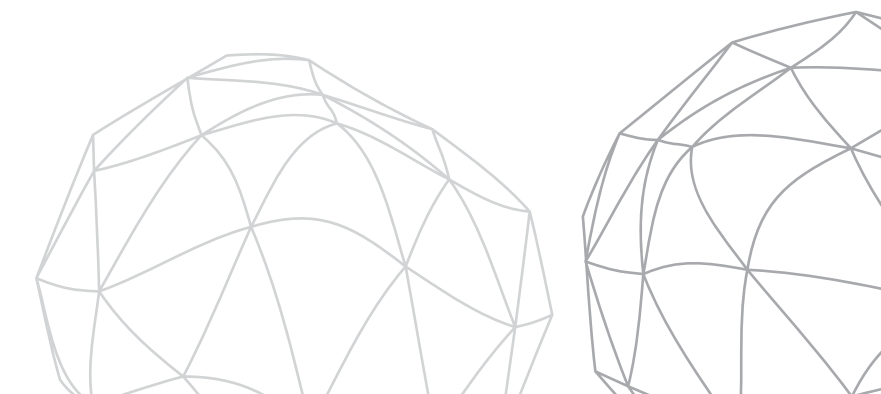
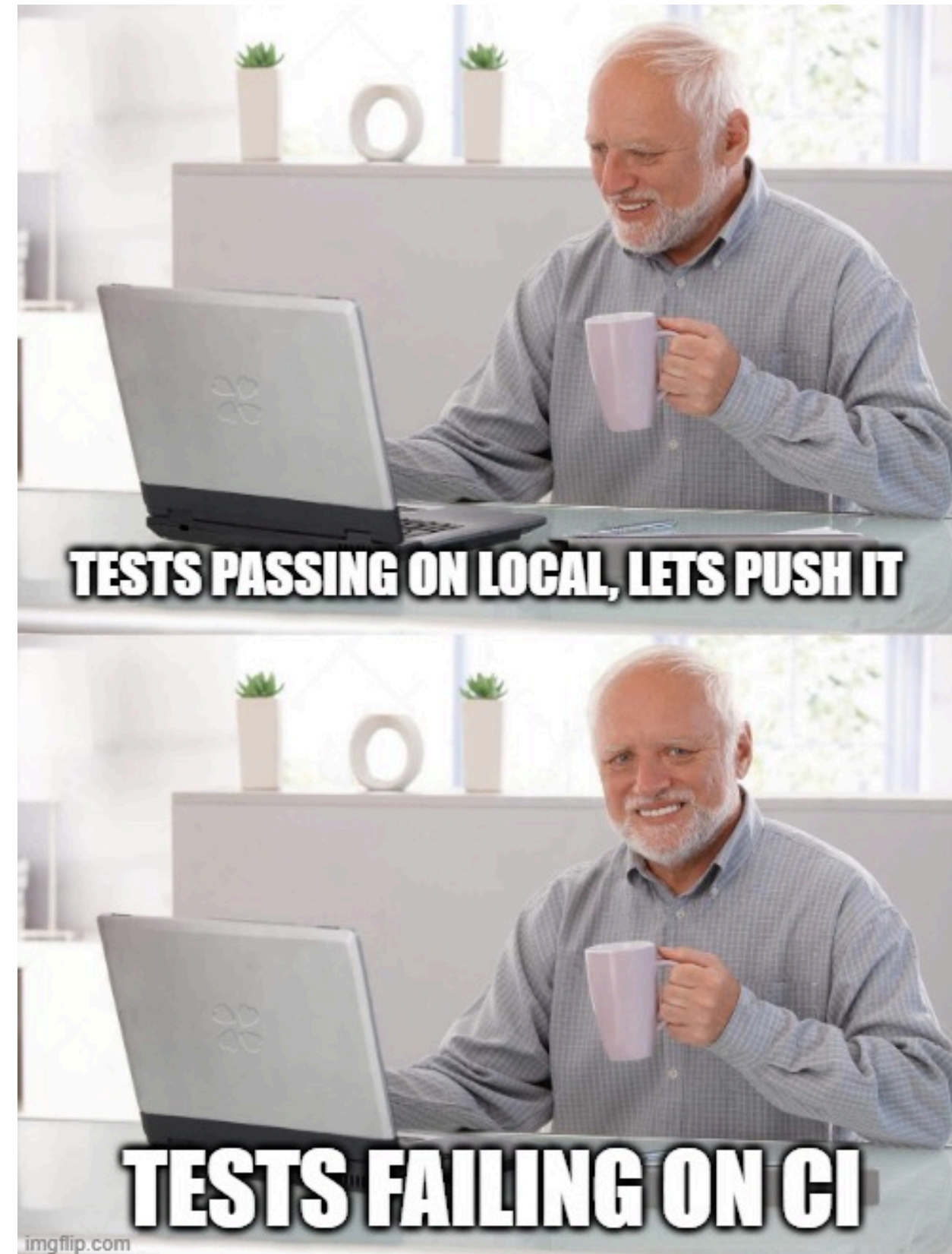


**Red Hat**

# What is CI/CD?



# CI Fails









# CI Fails



## Some checks were not successful

3 failing, 59 successful, and 2 skipped checks

[Hide all checks](#)

✗		<b>Lint Checks / lint (ubuntu-22.04, other) (pull_request)</b> Failing after 15m	Required	<a href="#">Details</a>
✗		<b>Python type checks / Run Mypy Type Checks (ubuntu-22.04) (pull_request)</b> Failing after 10m	Required	<a href="#">Details</a>
✓		<b>Backend associated test file check / Run backend associated test file checks (ubuntu-22.04) (pull_request)</b>	Required	<a href="#">Details</a>
✓		<b>Backend tests / Run backend tests (ubuntu-22.04, 1) (pull_request)</b> Successful in 24m	Required	<a href="#">Details</a>
✓		<b>Custom ESLint tests / Run Tests for Custom ESLint Checks (ubuntu-22.04) (pull_request)</b> Successful	Required	<a href="#">Details</a>
✓		<b>End-to-End coverage and Typescript test / e2e_coverage_and_typescript_tests (ubuntu-22.04) (pull_request)</b>	Required	<a href="#">Details</a>



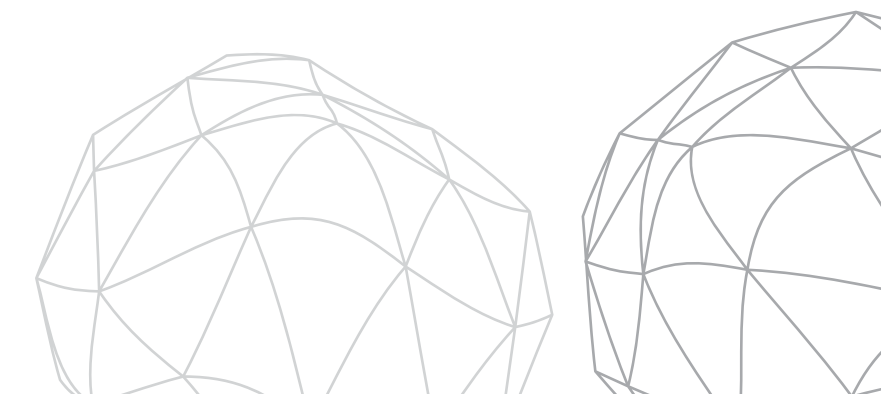
## This pull request is still a work in progress

Only those with [write access](#) to this repository can mark a draft pull request as ready for review.

# CI Fails

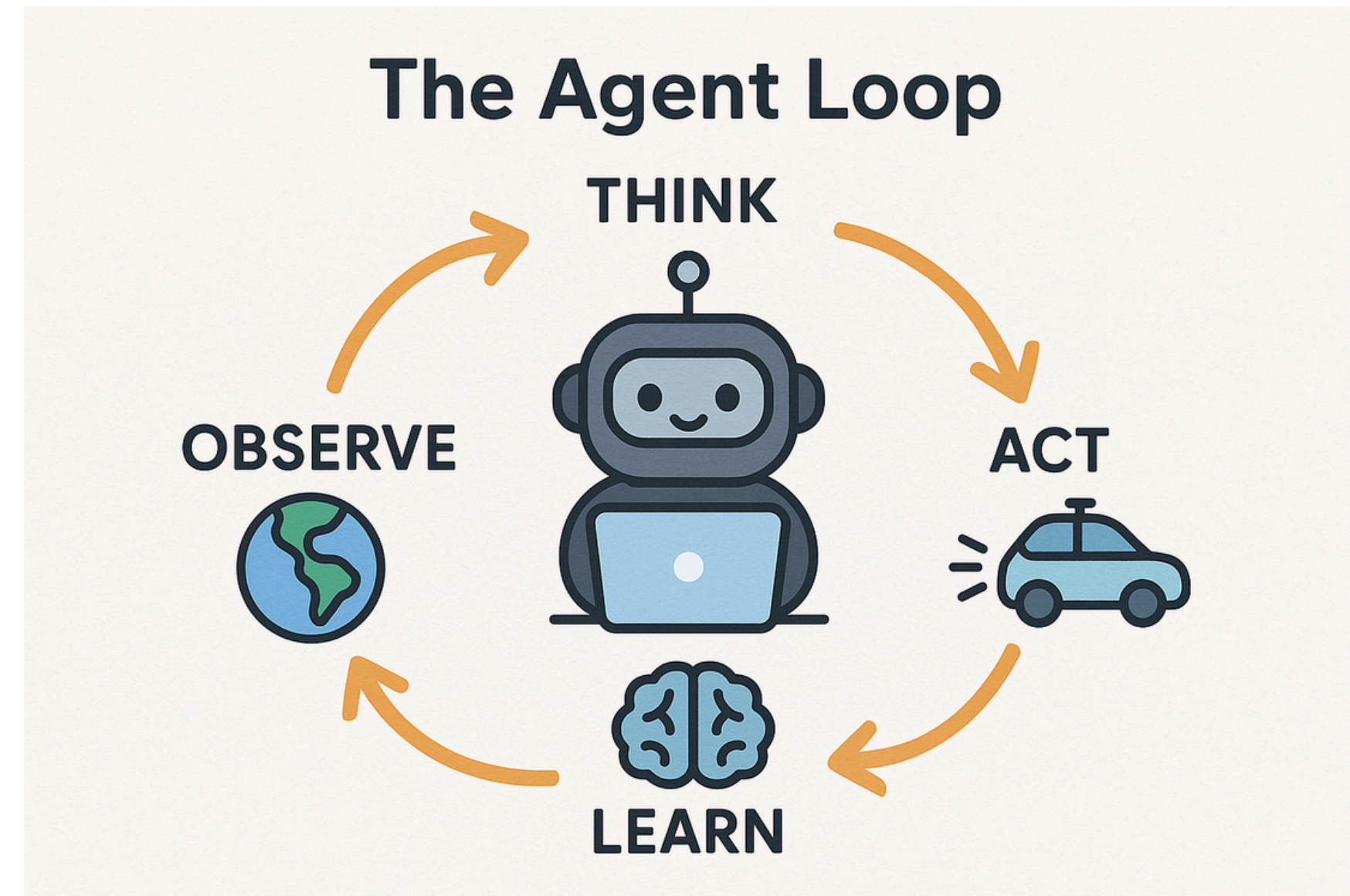
```
▼ ✓ Run tests on pCloudy 1m 15s
11169 [INFO] Running TestSuite
11170 [TestNGContentHandler] [WARN] It is strongly recommended to add "<!DOCTYPE suite SYSTEM "http://testng.org/testng-
1.0.dtd" >" at the top of your file, otherwise TestNG may fail or not work as expected.
11171 SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder".
11172 SLF4J: Defaulting to no-operation (NOP) logger implementation
11173 SLF4J: See http://www.slf4j.org/codes.html#StaticLoggerBinder for further details.
11174 [INFO ] 2020-07-15 05:45:05.342 com.automation.base.BaseClass:145 - log path:
logs/Android_MOTOROLA_MotoG5_Android_8.1.0
11175 java.lang.NullPointerException
11176 [ERROR] Tests run: 4, Failures: 1, Errors: 0, Skipped: 3, Time elapsed: 44.12 s <<< FAILURE! - in TestSuite
11177     at com.automation.listeners.TestListener.onTestSkipped(TestListener.java:87)
11178     at org.testng.internal.Invoker.runTestListeners(Invoker.java:1723)
11179 [ERROR] com.automation.tests.CICDTest.setUpQuizuPageClass Time elapsed: 43.594 s <<< FAILURE!
11180     at org.testng.internal.Invoker.runTestListeners(Invoker.java:1714)
11181 org.openqa.selenium.SessionNotCreatedException:
11182     at org.testng.internal.Invoker.registerSkippedTestResult(Invoker.java:1272)
11183 Unable to create a new remote session. Please check the server log for more details. Original error: Appium Server
Error due to some reason please check Hub/AppiumStdErr logs for more Information (WARNING: The server did not provide
any stacktrace information)
11184     at org.testng.internal.Invoker.invokeMethod(Invoker.java:605)
11185 Command duration or timeout: 41.34 seconds
11186     at org.testng.internal.Invoker.invokeTestMethod(Invoker.java:869)
11187 Build info: version: '3.14.0', revision: 'aaccce0', time: '2018-08-02T20:19:58.91Z'
11188     at org.testng.internal.Invoker.invokeTestMethods(Invoker.java:1193)
11189 System info: host: 'fv-az20', ip: '10.1.0.4', os.name: 'Linux', os.arch: 'amd64', os.version: '5.3.0-1032-azure',
java.version: '1.8.0_252'
11190     at org.testng.internal.TestMethodWorker.invokeTestMethods(TestMethodWorker.java:126)
11191 Driver info: driver.version: AndroidDriver
▶ ✓ Post Run actions/checkout@v2 0s
```

# Workflows can't fix themselves



# Agentic CI

**Agentic CI (Agentic Continuous Integration)** represents the next evolution of DevOps, moving from static, deterministic automation to autonomous, AI driven workflows.



# Self Healing CI/CD Pipeline

## Traditional CI/CD

- **Trigger:** Pipeline Fails.
- **Output:** Notification (Slack/Email).
- **Impact:** Engineering halts. Context switching for manual "Log Archaeology".
- **MTTR:** Measured in hours or days.

## Self Healing CI/CD

- **Trigger:** Pipeline Fails → Wakes Agent.
- **Output:** Automated PR + Root Cause Analysis.
- **Impact:** Self-correction in the background. Minimal developer interruption.
- **MTTR:** Measured in minutes.



**Some checks were not successful**

3 failing, 59 successful, and 2 skipped checks



**Pipeline Doctor: Auto-fix for main.py**

#6 opened last week by github-actions Bot

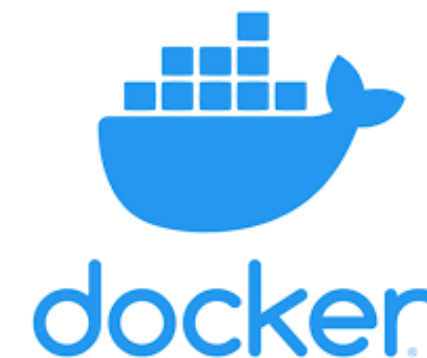
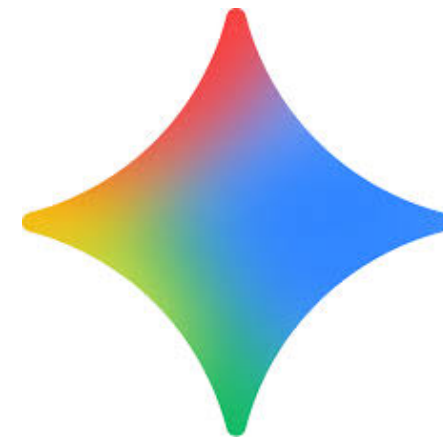
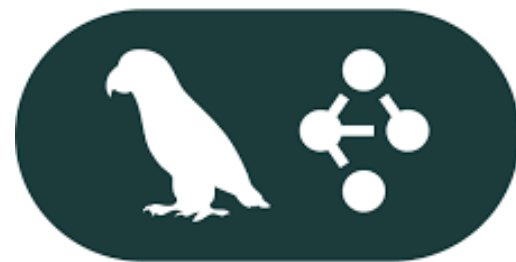
# Self Healing CI/CD Pipeline

## The Tech Stack

- **GitHub Actions** — Failure Detection & Trigger
- **LangGraph** — Agent Orchestration
- **Gemini** — Root Cause Analysis & Patch Generation
- **Docker** — Safe Validation Sandbox



GitHub Actions



# Self Healing CI/CD Pipeline

## Why Lang Graph?

### Nodes & Edges

- **Nodes** = Agent capabilities (Analyze, Patch, Validate)
- **Edges** = Decision logic and workflow routing

### Stateful Memory

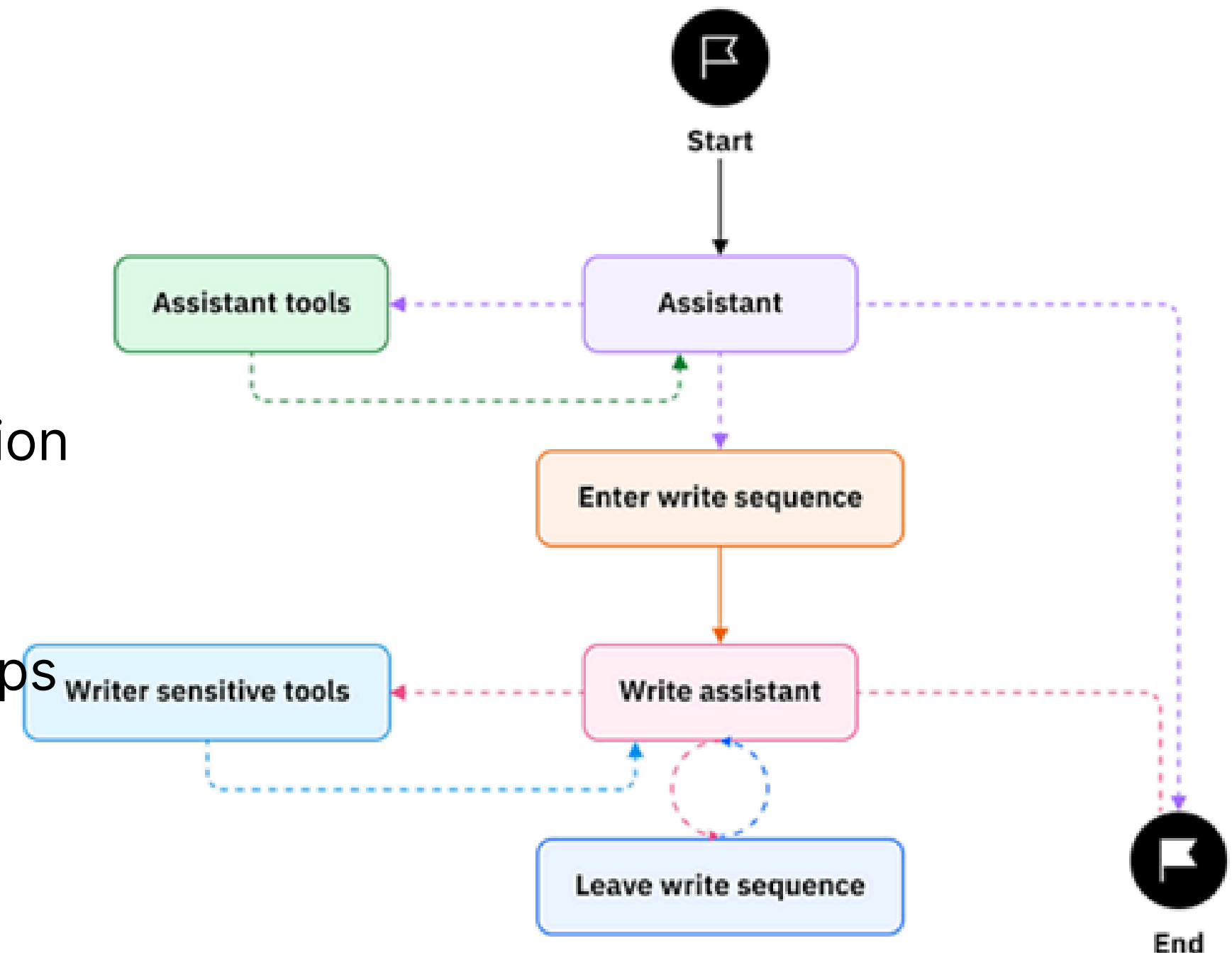
- Maintains context across the entire investigation
- Tracks findings, decisions, and actions

### Cyclical Workflows

- Supports Observe → Think → Act → Retry loops
- Unlike traditional linear pipelines

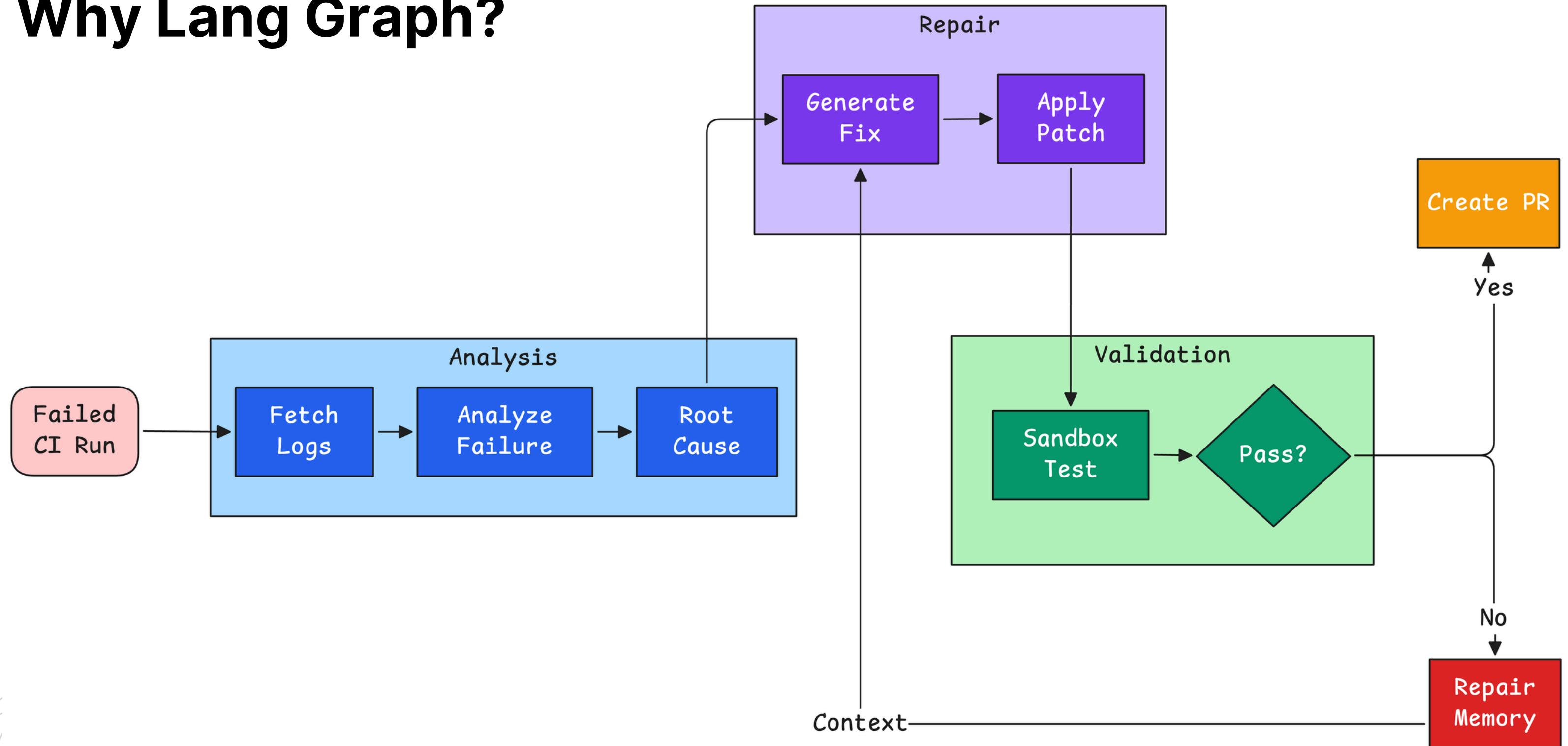
### Full Observability

- Every decision and transition is visible
- Easier debugging and auditing



# Self Healing CI/CD Pipeline

## Why Lang Graph?

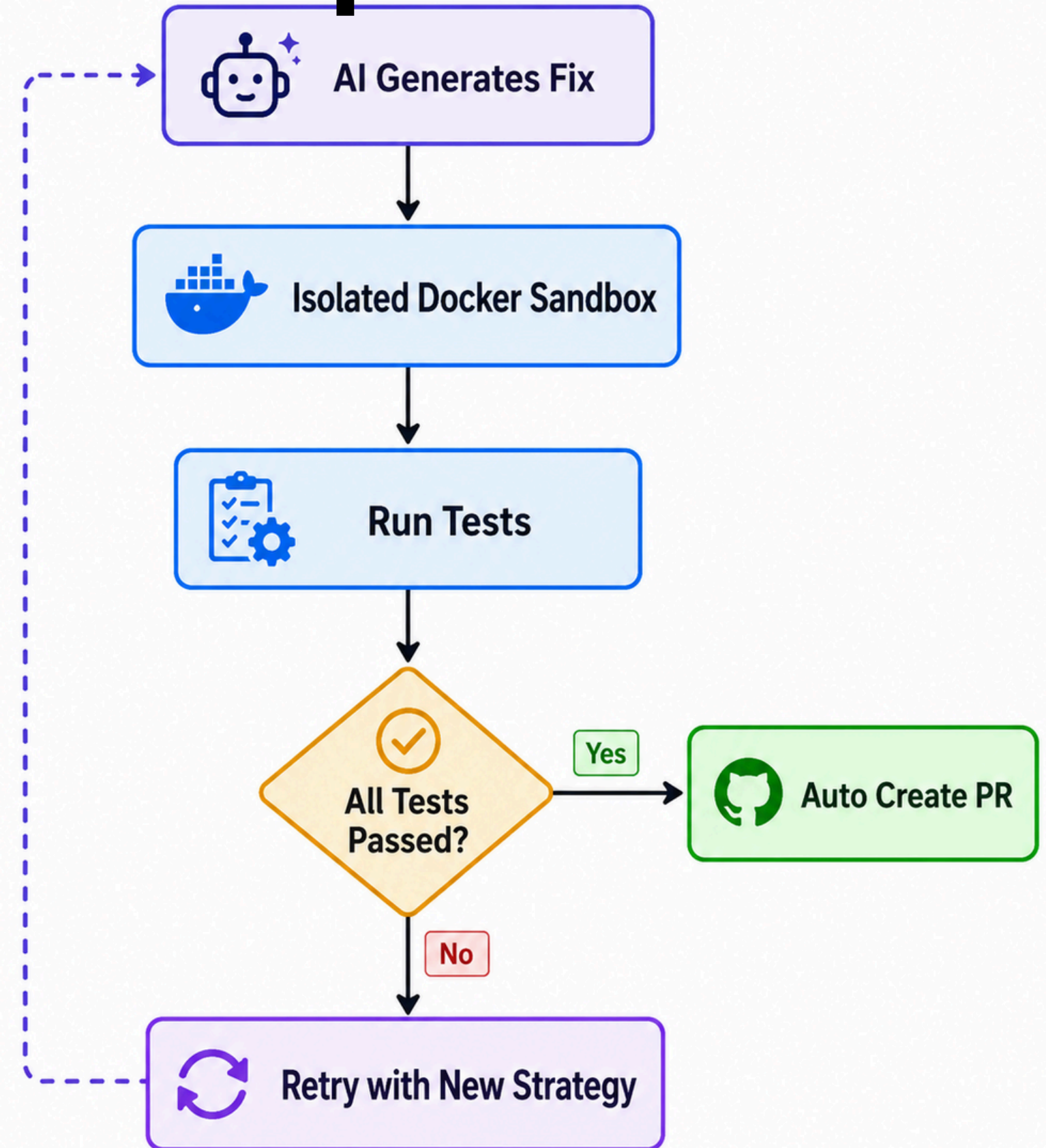


# Self Healing CI/CD Pipeline

## Sandbox Validation

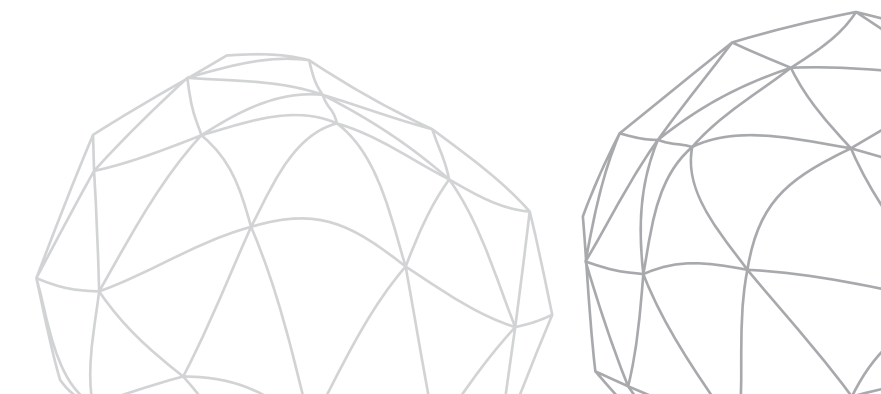
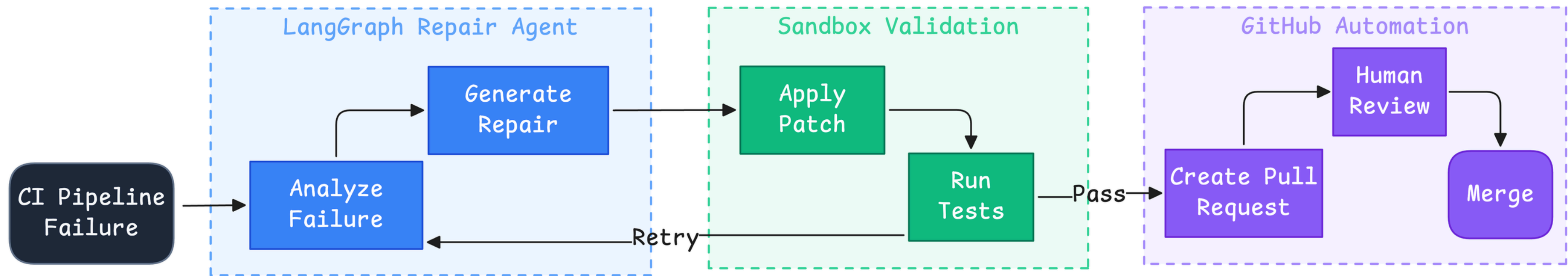
### Why?

- Prevent unsafe code execution
- Validate AI-generated patches
- Retry failed fixes automatically
- Only verified fixes become PRs



# Self Healing CI/CD Pipeline

## The Architecture



# Self Healing CI/CD Pipeline

## Safety & Governance

- Isolated Sandboxing

Agent-generated code is executed and validated in a secure, ephemeral Docker environment before integration.

- Human-in-the-Loop (HITL)

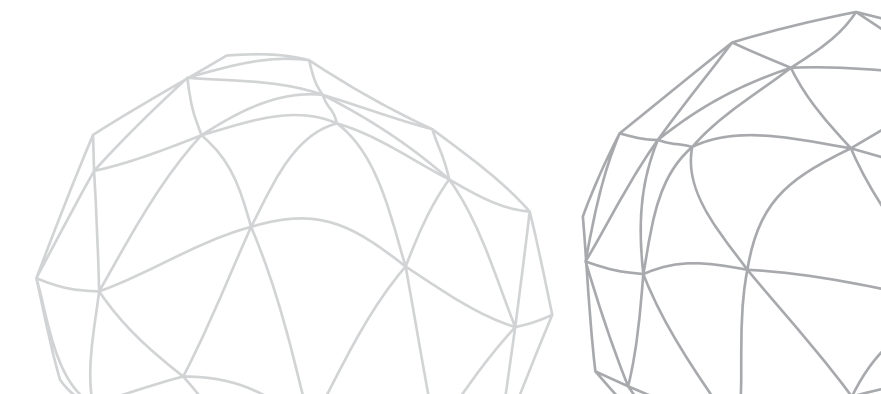
Agents propose fixes through Pull Requests. Human review and approval are required before changes are merged.

- Stateful Audit Trails

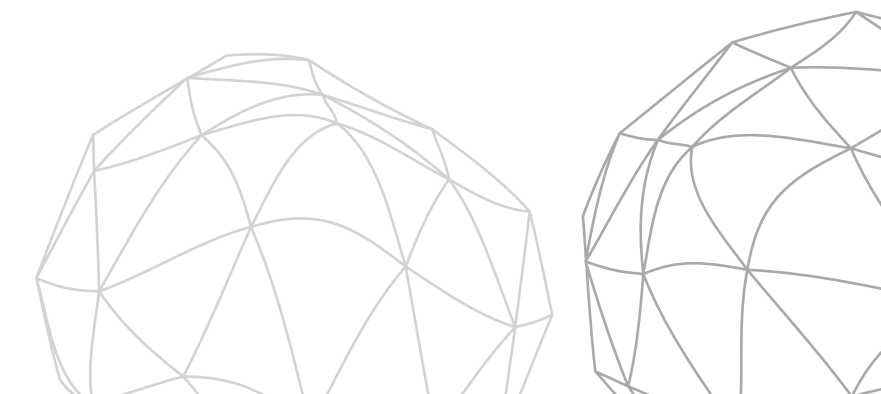
LangGraph orchestrates the agent workflow, providing transparent tracking of every decision, test run, and generated fix.

- Deterministic Validation

Automated regression checks ensure any proposed fix passes the entire existing test suite before reaching a reviewer.



# Self Healing CI/CD Pipeline



EXPLORER

- SELF ...
- \_\_pycache\_\_
- .github/workflows
  - ci.yml
  - doctor.yml
- .pytest\_cache
- .venv
- tests
- .gitignore
- agentic.py
- main.py**
- README.md
- requirements.txt
- sandbox.py

```

main.py
You, 11 hours ago | 1 author (You)
1 from fastapi import FastAPI, HTTPException
2 from pydantic import BaseModel, Field
3 from datetime import datetime, timezone
4 from typing import List, Optional
5
6 # Pydantic Models
You, 12 hours ago | 1 author (You)
7 class TodoCreate(BaseModel):
8     title: str = Field(..., min_length=1)
9     description: str = ""
10    completed: bool = False
11
You, 11 hours ago | 1 author (You)
12 class TodoUpdate(BaseModel):
13     title: Optional[str] = None
14     description: Optional[str] = None
15     completed: Optional[bool] = None
16
You, 12 hours ago | 1 author (You)
17 class Todo(BaseModel):
18     id: int
19     title: str
20     description: str
21     completed: bool
  
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS GITLENS

(.venv) premveddhote@Premveds-MacBook-Air Self Healing Agentic CICD %

- OUTLINE
- TIMELINE
- SNIPPETS

# Thank You!

**Premved Dhote**

**Software Engineering Intern**



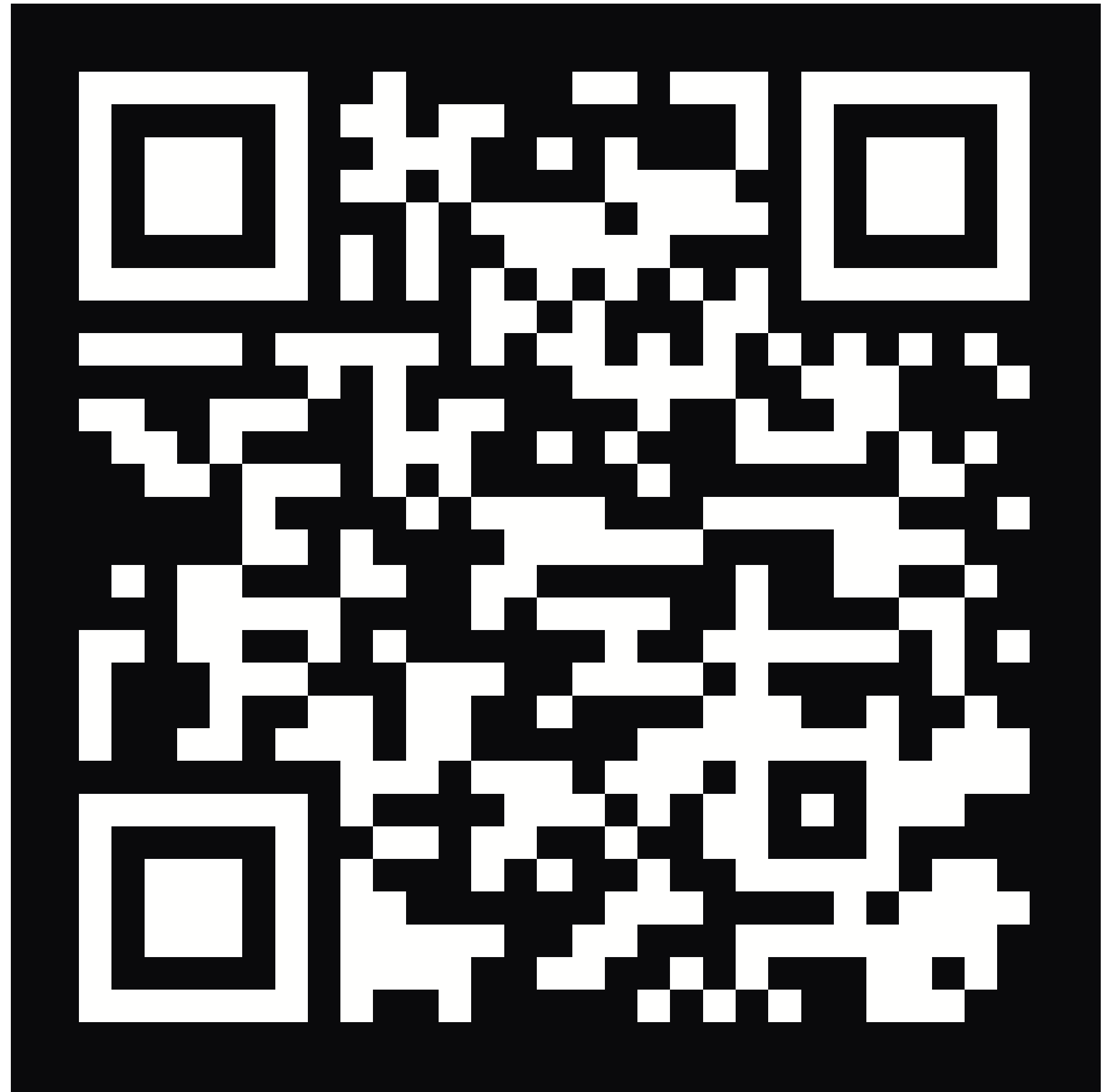
**Red Hat**



premveddhote



@PVDIUM



**SCAN FOR ALL LINKS**