About Us

NICOLE SCHULTZ
Asst. Director, Engineering

BOBBI WENZLER
Lead Product Manager

Northwestern Mutual

Headquartered in Milwaukee, WI
Additional offices in Franklin, WI and New York, NY

Northwestern Mutual

FOR 165 YEARS,

NORTHWESTERN

MUTUAL

HAS BEEN HELPING

FAMILIES AND

BUSINESSES ACHIEVE

FINANCIAL SECURITY

Revenue **$34 billion**

#97 on FORTUNE 500

4.9+ Million Clients

97% of clients stay with us year over year*

7,600+ Employees

Northwestern Mutual®

Beginning the Climb

THE PROBLEM

24,000+ codebases and growing.
15,000+ pipelines run every day.

Standards manually captured in a library of de-centralized documentation

Feedback only occurring far right in the dev process. Show up on audit reports months after a release.

Manual follow-up and tracking on resolution of compliance findings.

WHERE WE STARTED

Gathering data

Cross-functional alignment with leadership

Developing a proof-of-concept enforcement mechanism

Communication & runway

Northwestern Mutual®

Continuing Our Ascent: Pipeline Enforcer

Pipeline Enforcer: NM-built product that provides guardrails on security, audit & quality practices

Compliance guardrails now maintained programmatically instead of in documents

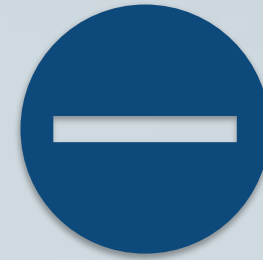Shifts feedback left in for earlier resolution

Moves the needle on resolution of standardized compliance checks in pipelines

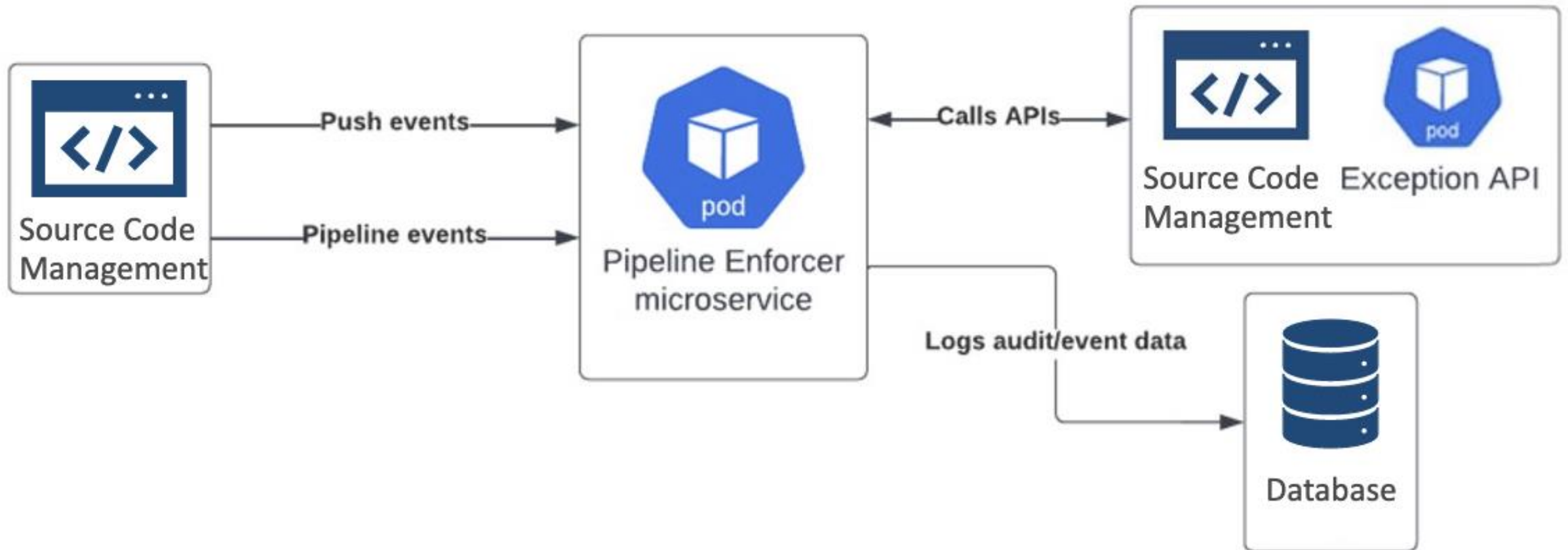# Continuing Our Ascent: Maintaining the Developer Experience

Warnings

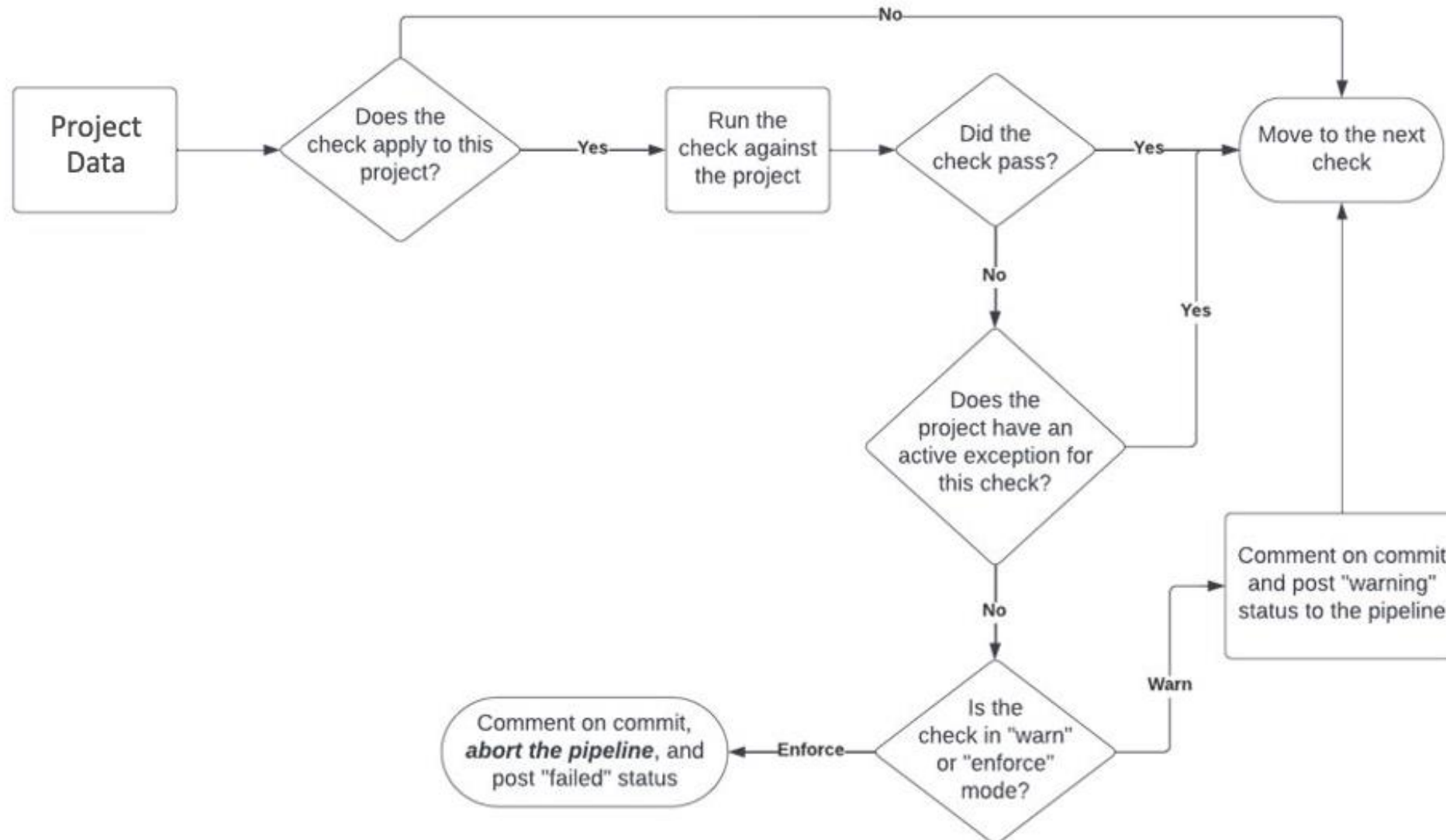Allow ample runway for adoption

Real-time feedback for resolution

Short-Term Exceptions

To account for production outages

Require approvals

Pipeline Enforcer Architecture

Anatomy of a Check

Warning on a Pipeline

.pre
- ✅ Code Linting ⟳
- ✅ Code Security ⟳
- ✅ Dead Code ⟳
- ✅ Dependency ... ⟳
- ✅ Dockerfile Li... ⟳
- ✅ SAST ⟳

Build
- ✅ Build ⟳

Scans
- ✅ Container Sc... ⟳

Deploy non-prod
- ✅ Deploy Non-... ⟳

External
- ✅ [Warning] - Pip...

[Warning] - Pipeline Enforcer - See linked comment(s) for details.

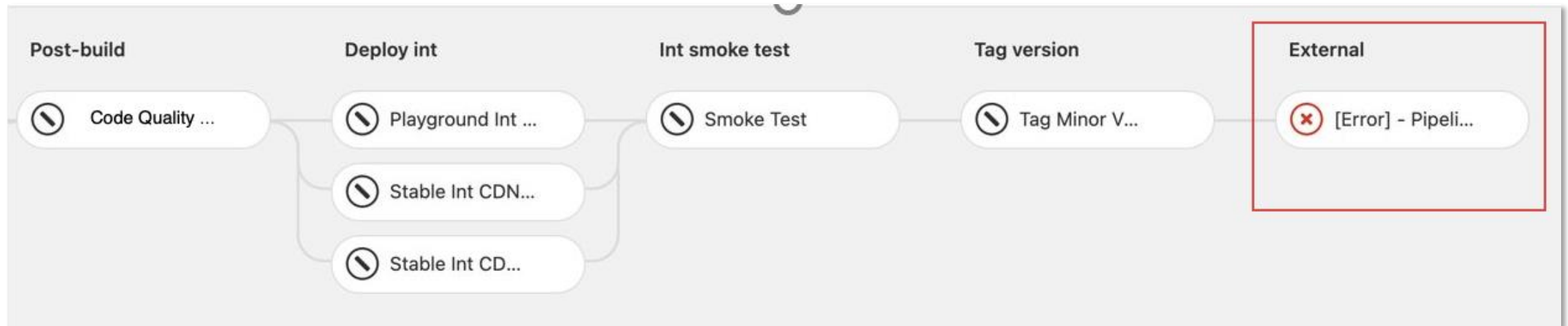**Pipeline Enforcer** @pipeline-enforcer · 5 months ago

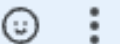The following issues were found with the build pipeline for this commit:

- **Code Quality Scanning**
  - ⚠️ **WARNING** ⚠️ This project contains a language that should have code quality scanning. This is a **mandatory** requirement and this pipeline will be cancelled starting on **MM/DD/YYYY.**
  - **TAKE ACTION NOW**: By adding code quality scanning to your pipeline.

Enforcement – Cancelling a Pipeline

Post-build

- Code Quality ...

Deploy int

- Playground Int ...
- Stable Int CDN...
- Stable Int CD...

Int smoke test

- Smoke Test

Tag version

- Tag Minor V...

External

- [Error] – Pipeli...

Pipeline Enforcer @pipeline-enforcer · 11 minutes ago

The following issues were found with the build pipeline for this commit:

- **Static Application Security Testing (SAST)**
    - ○ 🚨 **FAILURE** 🚨 This pipeline is not stopping when this project has high severity Static Application Security Testing (SAST) vulnerabilities. This is a **mandatory** requirement and this pipeline has been **cancelled**.
    - ○ **TAKE ACTION NOW**: By removing `allow_failure: true` from your SAST job OR changing it to `allow_failure: false` and handling any high severity vulnerabilities.
    - ○ **NEED AN EXCEPTION?**:go here!

Requesting Exceptions (Standard Process)

Requesting Exceptions (P1/P2 outage)

Continuing Our Ascent: What Are We Enforcing?

Security

Code Quality

Peer Review

Victory!

Pipelines Require Code Reviews
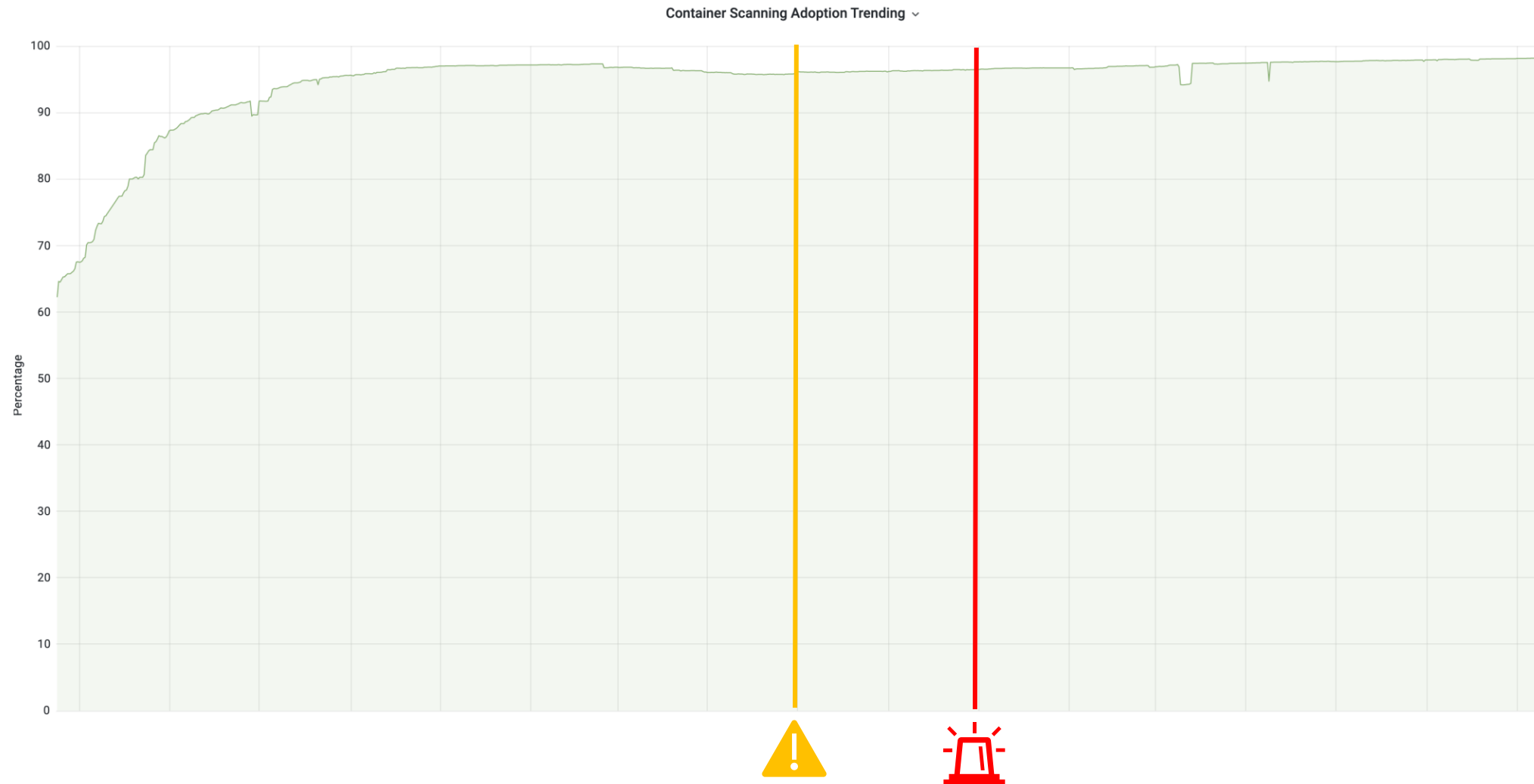

Trend of Projects where MRs Require Approval
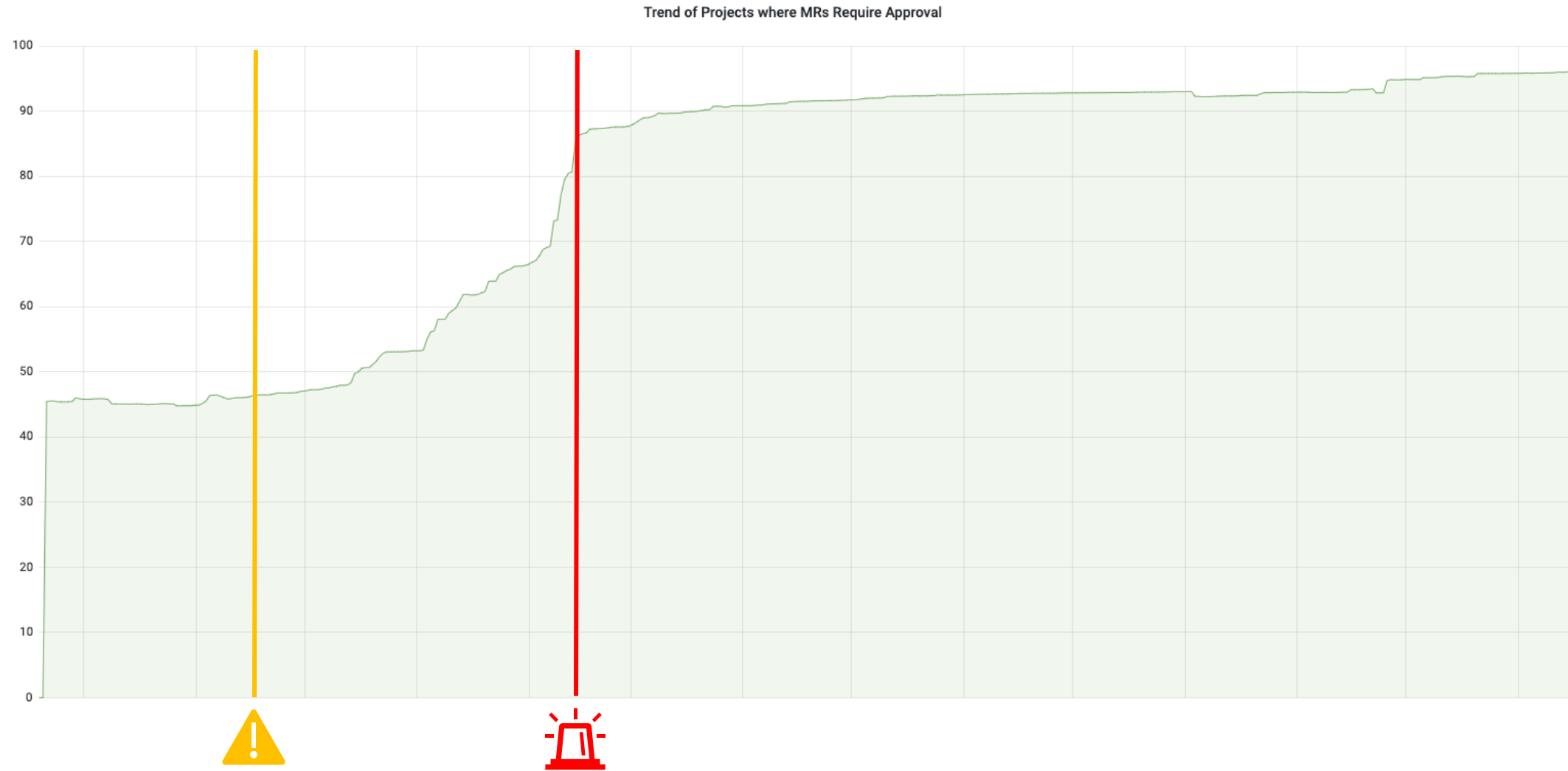
Pipelines Require Static Security Jobs to Fail

Static Scanning stopping on failures Trending
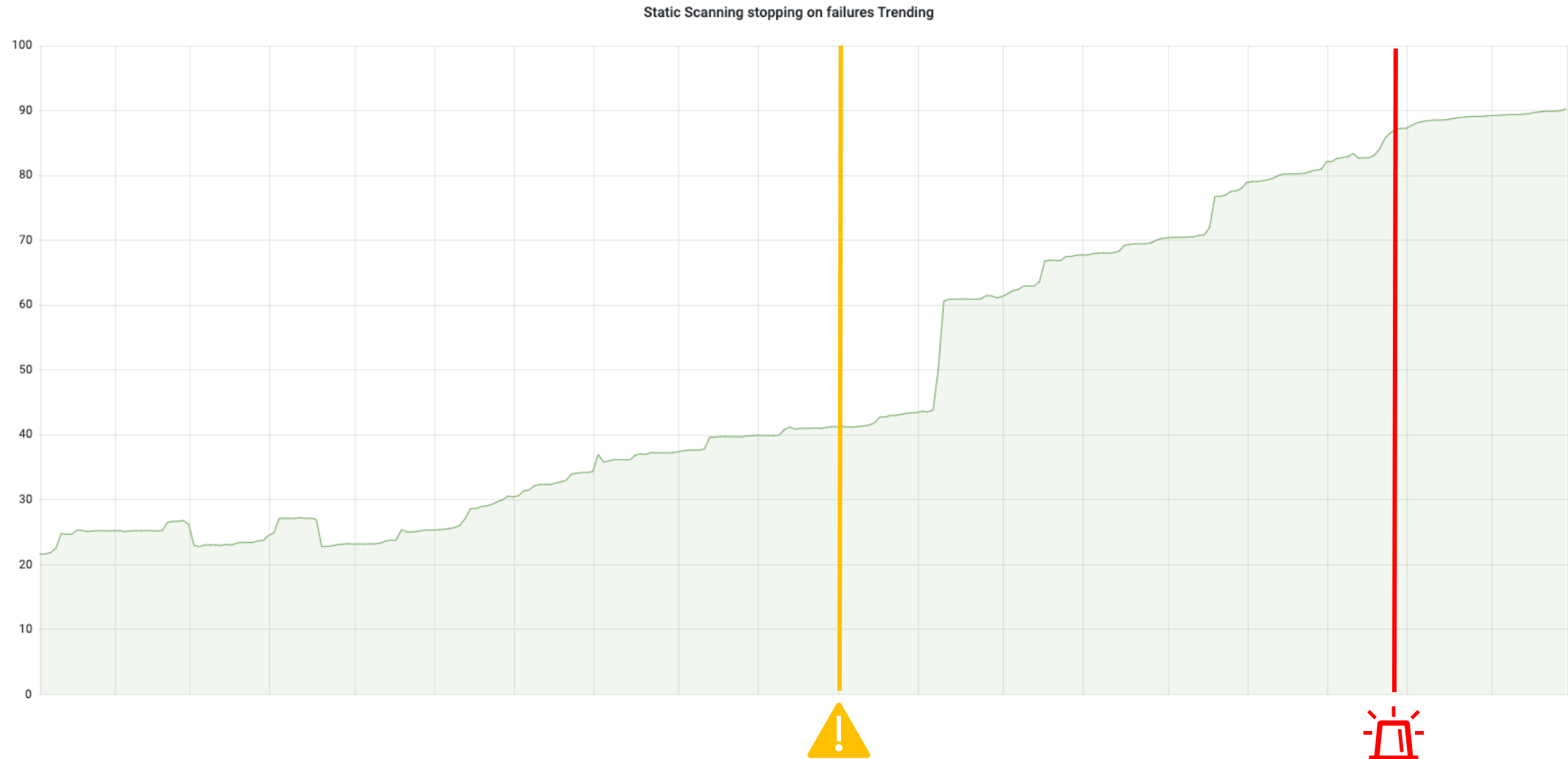
Pipelines Require Code Quality Scanning

Code Quality Analysis ˅
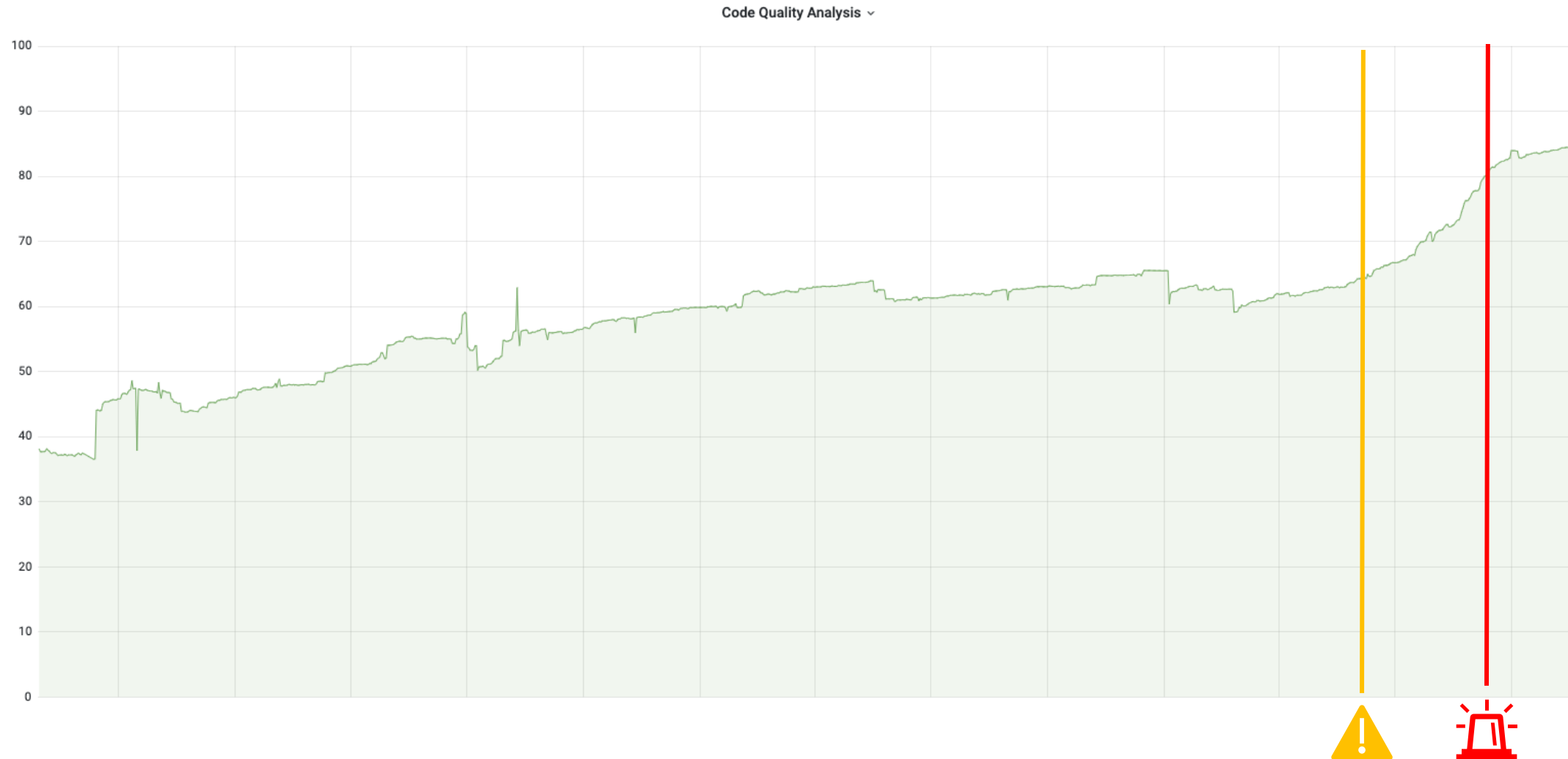
Pipelines Require Container Scanning

Container Scanning Adoption Trending

What's on the Horizon?

[Standardized, opinionated pipelines]

[Automated Day 2 Operations]

[Providing a holistic visual of compliance findings at application level]

THANK YOU

Northwestern Mutual®