

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

FOR 165 YEARS,
NORTHWESTERN
MUTUAL
HAS BEEN HELPING
FAMILIES AND
BUSINESSES ACHIEVE
FINANCIAL SECURITY

*Loyalty is based on Northwestern Mutual client data.

© 2022 The Northwestern Mutual Life Insurance Company. All Rights Reserved.



Revenue **\$34 billion**

#97 on FORTUNE 500


4.9+ Million Clients


97% of clients stay with us
year over year*


7,600+ Employees

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

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



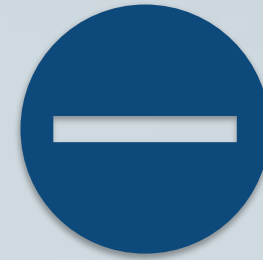
Moves the needle on resolution of standardized compliance checks in pipelines

Continuing Our Ascent: Maintaining the Developer Experience



Warnings

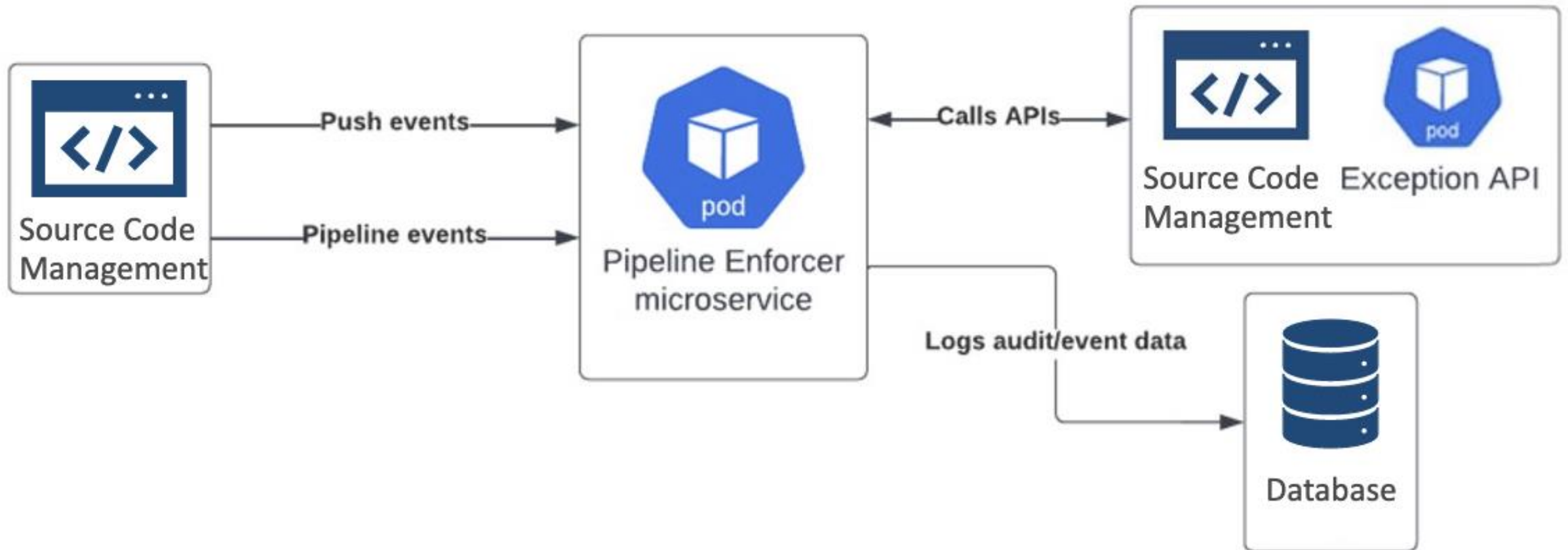
Allow ample runway for adoption
Real-time feedback for resolution



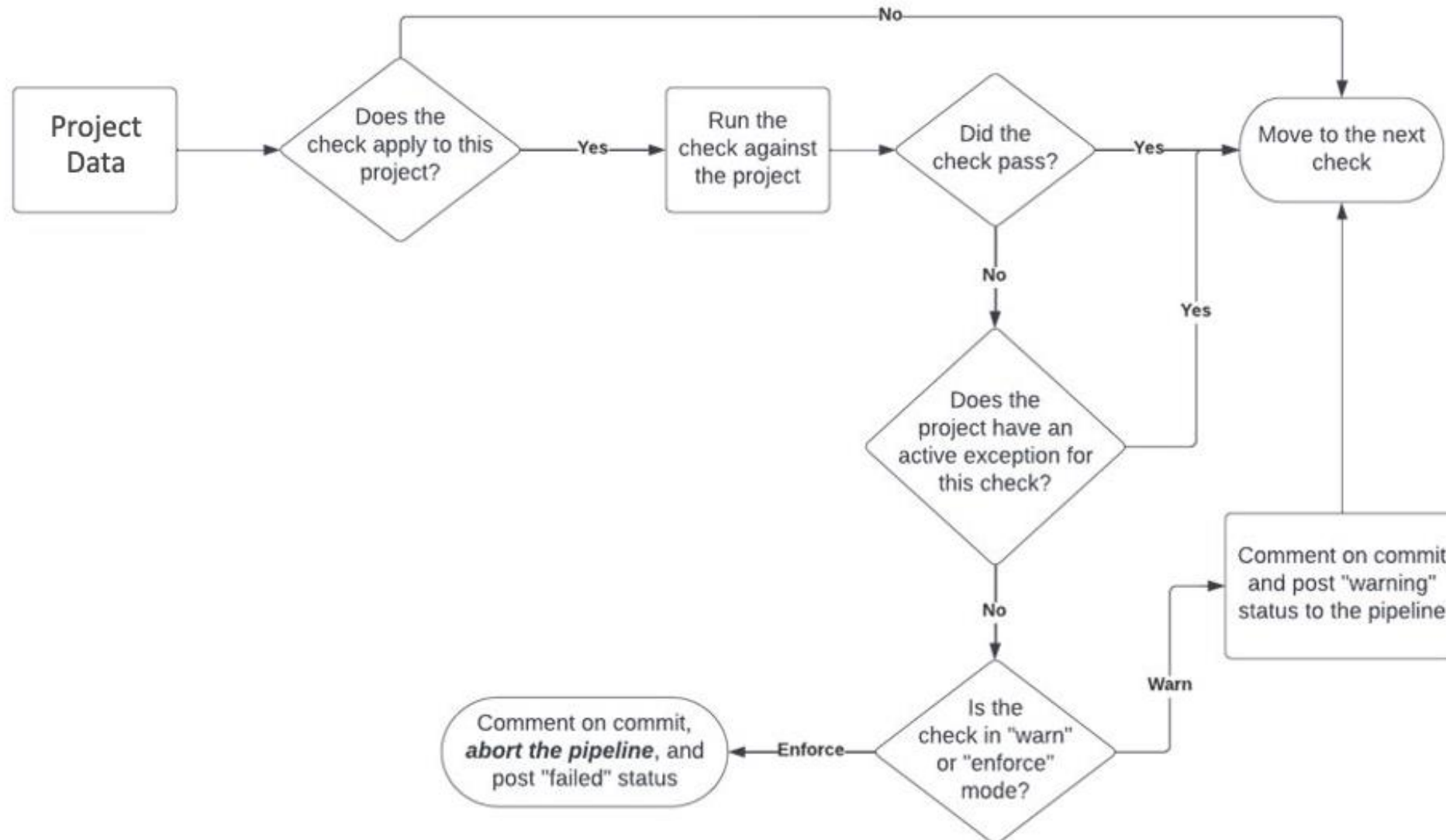
Short-Term Exceptions

To account for production outages
Require approvals

Pipeline Enforcer Architecture



Anatomy of a Check



Warning on a Pipeline

The screenshot displays a pipeline dashboard with the following stages and items:

- .pre**: Code Linting, Code Security, Dead Code, Dependency ..., Dockerfile Li..., SAST.
- Build**: Build.
- Scans**: Container Sc...
- Deploy non-prod**: Deploy Non-...
- External**: [Warning] - Pip...

A red box highlights the 'External' section, which contains a warning message: "[Warning] - Pipeline Enforcer - See linked comment(s) for details." A tooltip points from the warning item to this message.



Pipeline Enforcer @pipeline-enforcer · 5 months ago

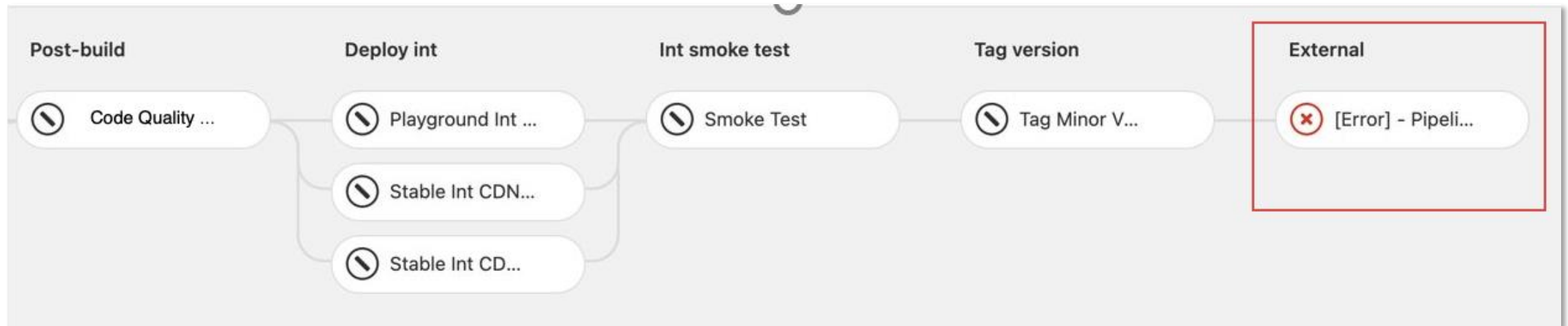


The following issues were found with the build pipeline for this commit:

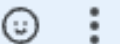
- **Code Quality Scanning**

- **⚠ 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



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)

The screenshot shows a web application interface for requesting exceptions. A modal titled "Request Exceptions" is open, displaying the following fields and options:

- Repository***: A text input field containing "cicd/devops-api".
- Select approvers to notify via Slack (up to 5)**: A dropdown menu showing "Schultz, Nicole" with a close icon.
- Exception 1**: A section containing:
 - Exception Type***: A dropdown menu showing "Merge Request Self Approvals".
 - Reason***: A dropdown menu showing "Sunsetting".
 - Expiration Date***: A date input field showing "2022-12-11".
 - Comment (optional)**: A text area for additional comments.
- + ADD ANOTHER EXCEPTION**: A button to add more exceptions.
- SUBMIT**: A button to submit the request.

The background interface includes a sidebar with navigation links (Projects, DL-CICD-ENG, #cicd-support), a top navigation bar with a search bar and filters (PENDING (0), APPROVED (0), DENIED (0), EXPIRED/RETIRED (4)), and a main content area showing project details for "devops-api".

Requesting Exceptions (P1/P2 outage)

Exception

NAVIGATION

Projects

EXTERNAL LINKS

our-email

#our-slack

Created by
Infrastructure &
Cloud Services

Bobbi Wenzler

Projects

group/project

PENDING (0)

APPROVED (0)

DENIED (0)

EXPIRED/RETIRED (4)

REQUEST NEW EXCEPTION

Repository
group/project

Asset
Our Asset

UTAN
special UTAN

Asset Owner
Nicole Schultz

Engineering Lead
Our Lead is Awesome!

Top Tier
No

Default Branch
master

Your Access Level
Developer

Approvers

VIEW APPROVERS LIST

Request Exceptions

SUBMIT

Repository*

group/project

Select approvers to notify via Slack (up to 5)

Exception 1

Exception Type*

Merge Request Self Approvals

Reason*

Recovering from a system outage (P1 or P2 only)

Expiration Date*

2022-11-13

Incident Number*

Please enter an incident number (e.g. INC0001234)

Comment (optional)

+

ADD ANOTHER EXCEPTION

Continuing Our Ascent: What Are We Enforcing?



Security



Code Quality

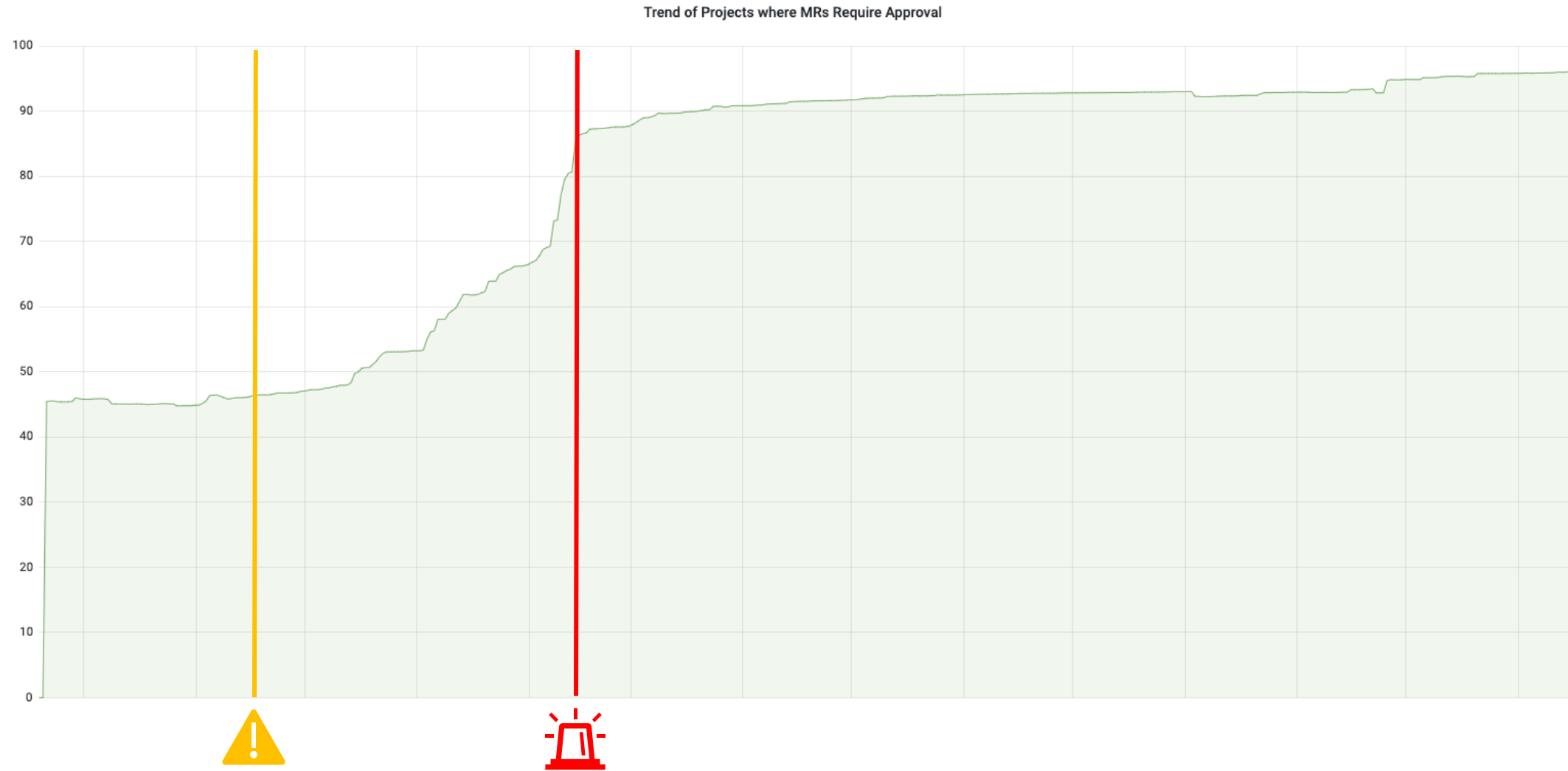


Peer Review

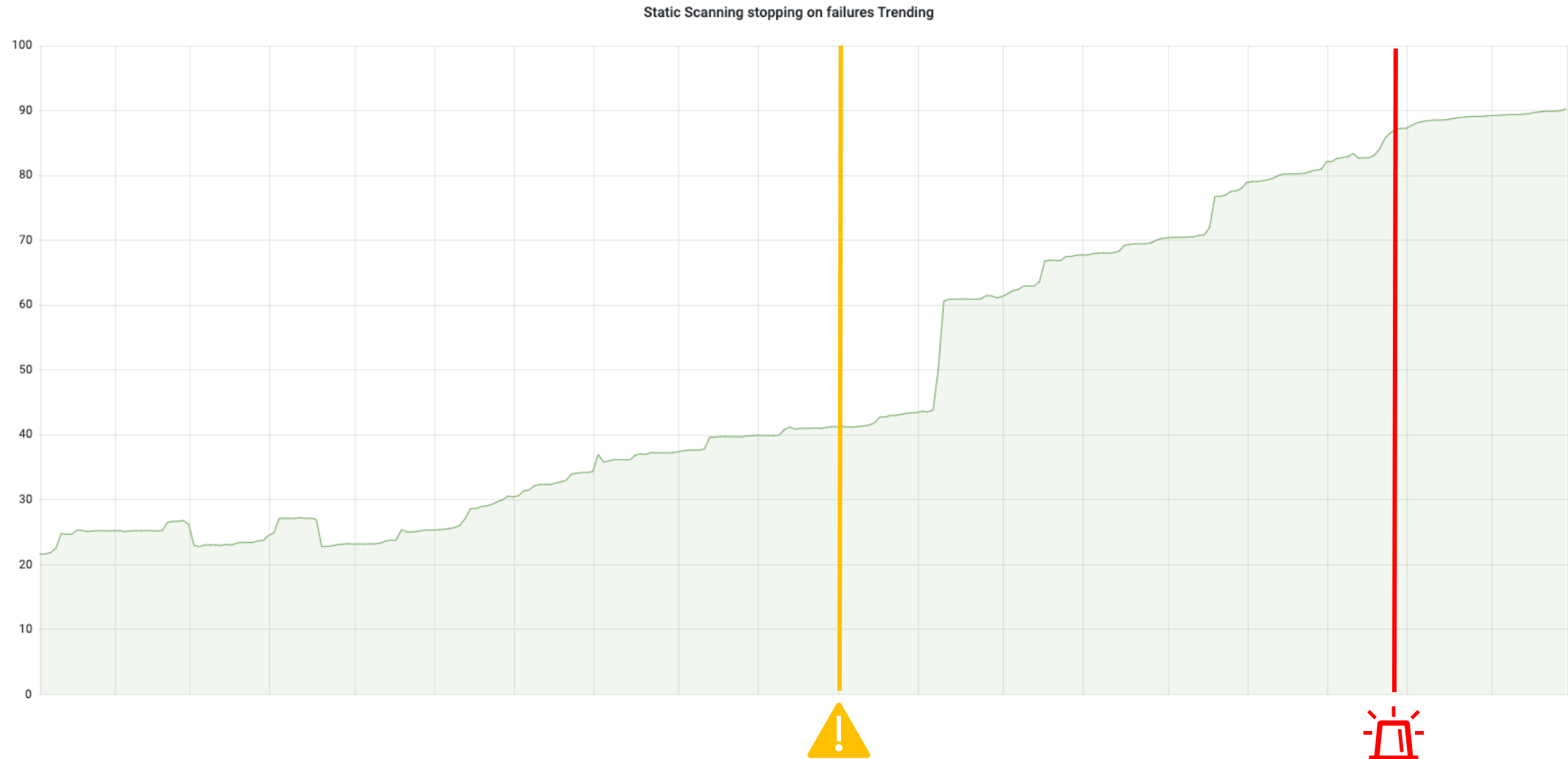
Victory!



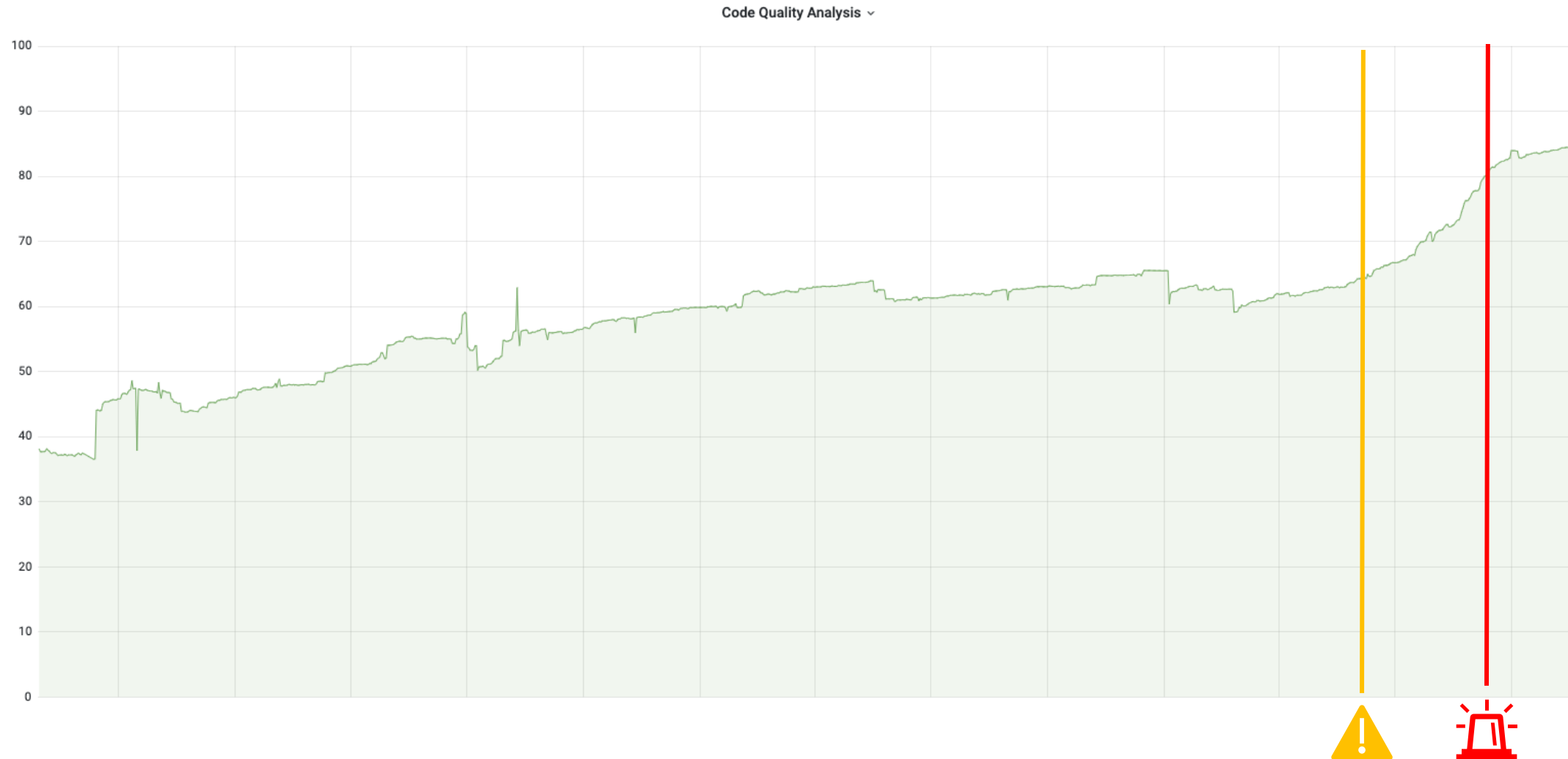
Pipelines Require Code Reviews



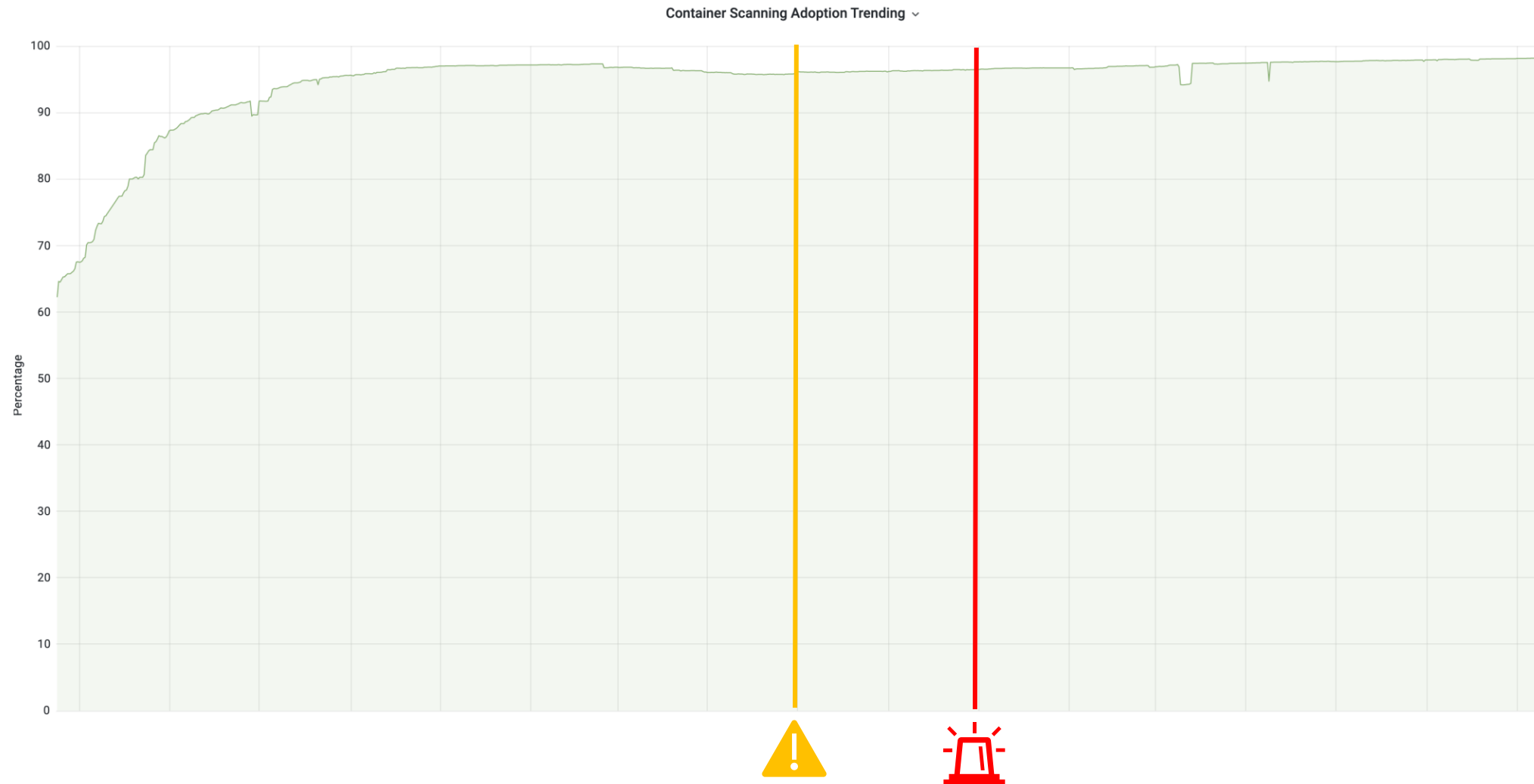
Pipelines Require Static Security Jobs to Fail



Pipelines Require Code Quality Scanning



Pipelines Require Container Scanning



What's on the Horizon?

Standardized, opinionated
pipelines

Automated Day 2
Operations

Providing a holistic visual
of compliance findings at
application level

THANK YOU

