

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



Revenue **\$34 billion**

#97 on FORTUNE 500

4.9+ Million Clients

97% of clients stay with us
year over year*

7,600+ Employees

*Loyalty is based on Northwestern Mutual client data.

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

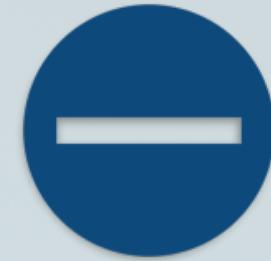
Continuing Our Ascent: Maintaining the Developer Experience



Warnings

Allow ample runway for adoption

Real-time feedback for resolution

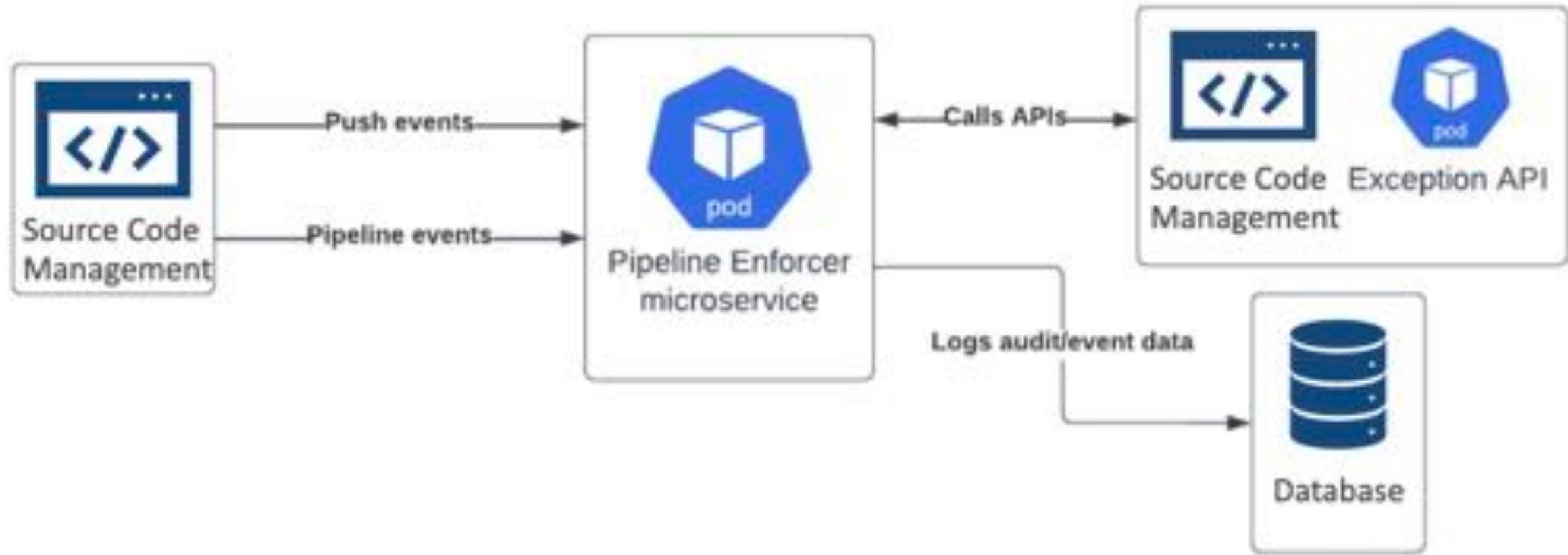


Short-Term Exceptions

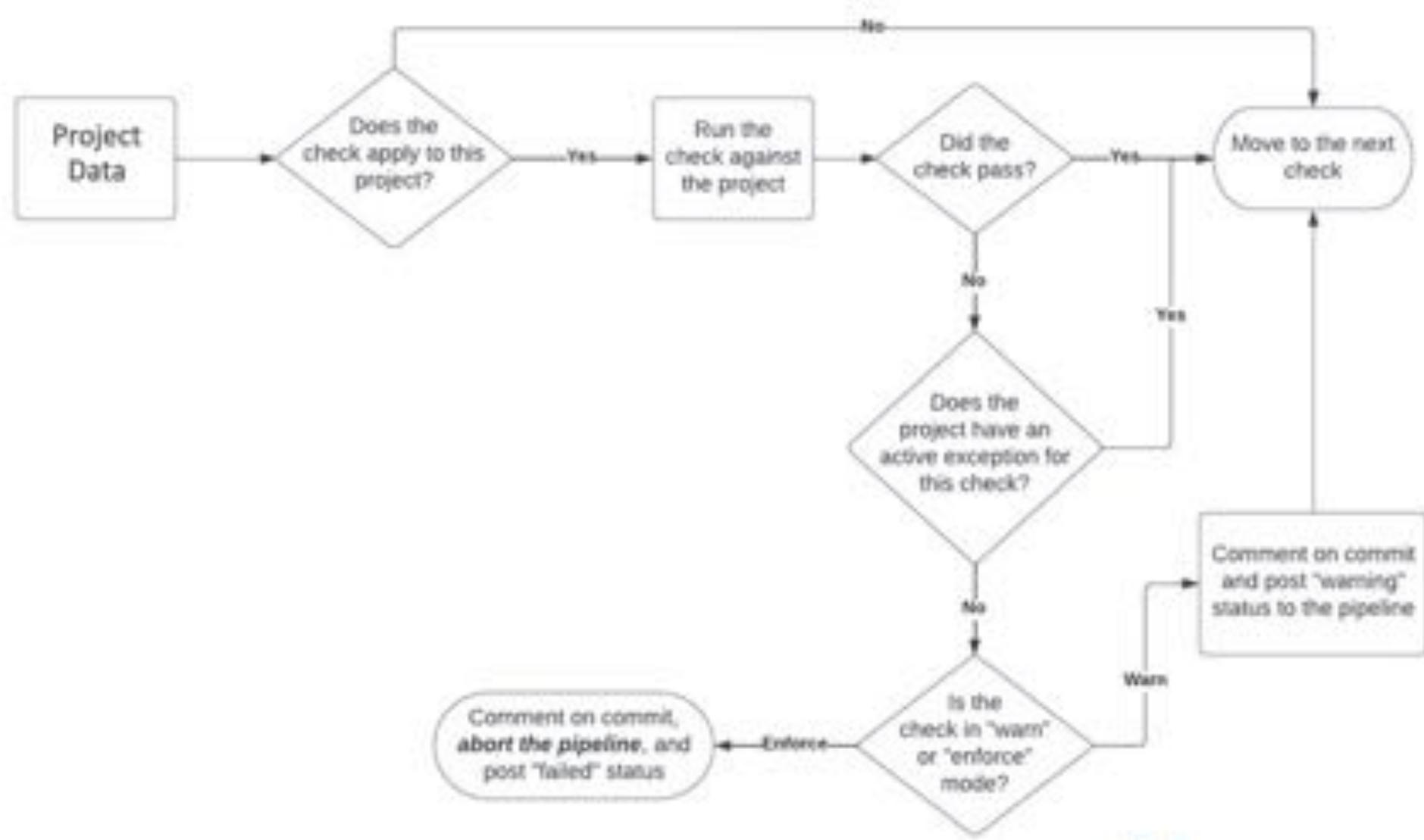
To account for production outages

Require approvals

Pipeline Enforcer Architecture



Anatomy of a Check



Warning on a Pipeline

The screenshot shows a pipeline interface with several stages: pre, Build, Scans, Deploy non-prod, and External. The External stage is highlighted with a red border and contains a warning message from 'Pipeline Enforcer'.

External

[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



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 software interface for managing exceptions. A modal window titled "Request Exceptions" is open in the foreground, prompting the user to enter details for a new exception. The modal includes fields for "Exception Type" (set to "Merge Request Self Approval"), "Reason" (set to "Sunsetting"), and "Expiration Date" (set to "2022-12-11"). Below these fields is a "Comment" input field and a "Submit" button. In the background, a "Projects" page is visible, featuring a sidebar with various filters like "Project", "Status", "Type", and "Priority". The main area of the page shows a list of items with columns for "Title", "Status", and "Last Updated". A navigation bar at the top includes tabs for "PENDING", "APPROVED", "DENIED", and "EXPIRED/REMOVED".

Requesting Exceptions (P1/P2 outage)

The screenshot shows a software interface for managing exceptions. On the left, there's a sidebar with various project and system management links. The main area is titled 'Request Exceptions' and contains three tabs: 'Exception' (selected), 'Approval', and 'Comments'. The 'Exception' tab displays a form with the following fields:

- Exception Type:** Recovering from a system outage (P1 or P2 only) (highlighted by a red box)
- Expiration Date:** 2023-11-13 (highlighted by a red box)
- Incident Number:** # (Placeholder: Please enter an incident number (e.g. 98C0001234))
- Comment:** (Placeholder: Enter comment)

At the bottom of the form is a button labeled 'ADD ANOTHER EXCEPTION'.

Continuing Our Ascent: What Are We Enforcing?



Security



Code Quality



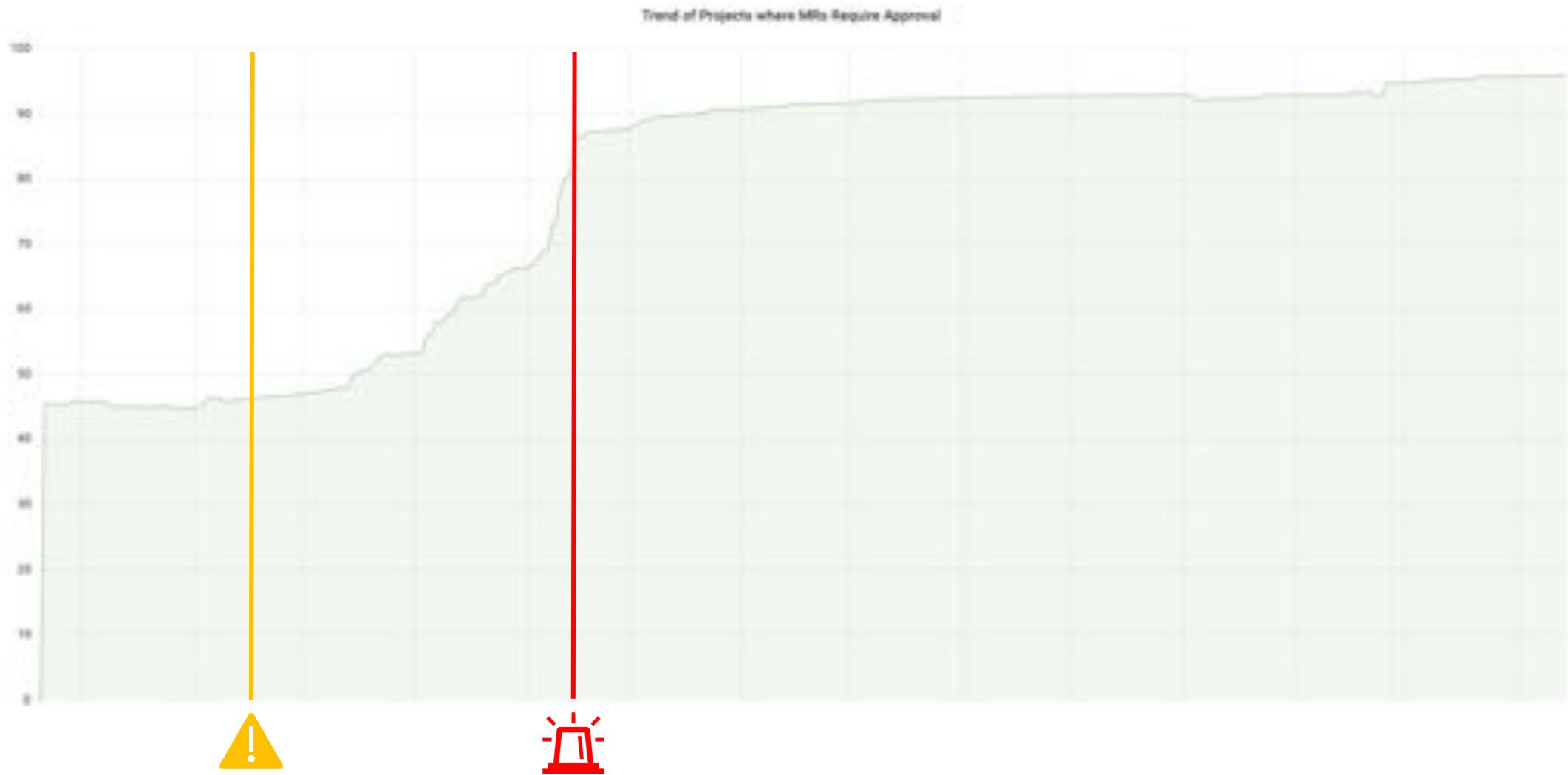
Peer Review



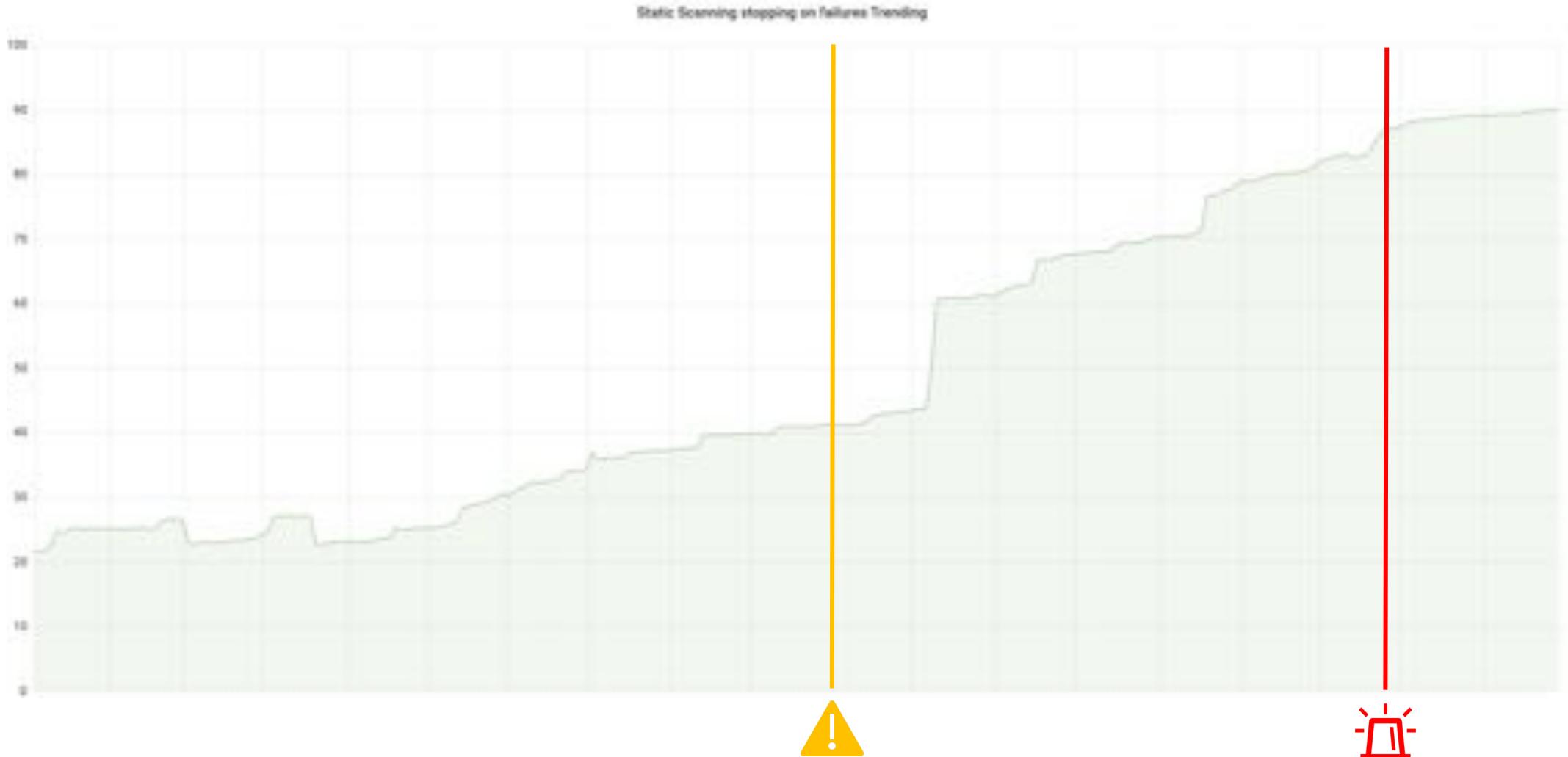
Victory!



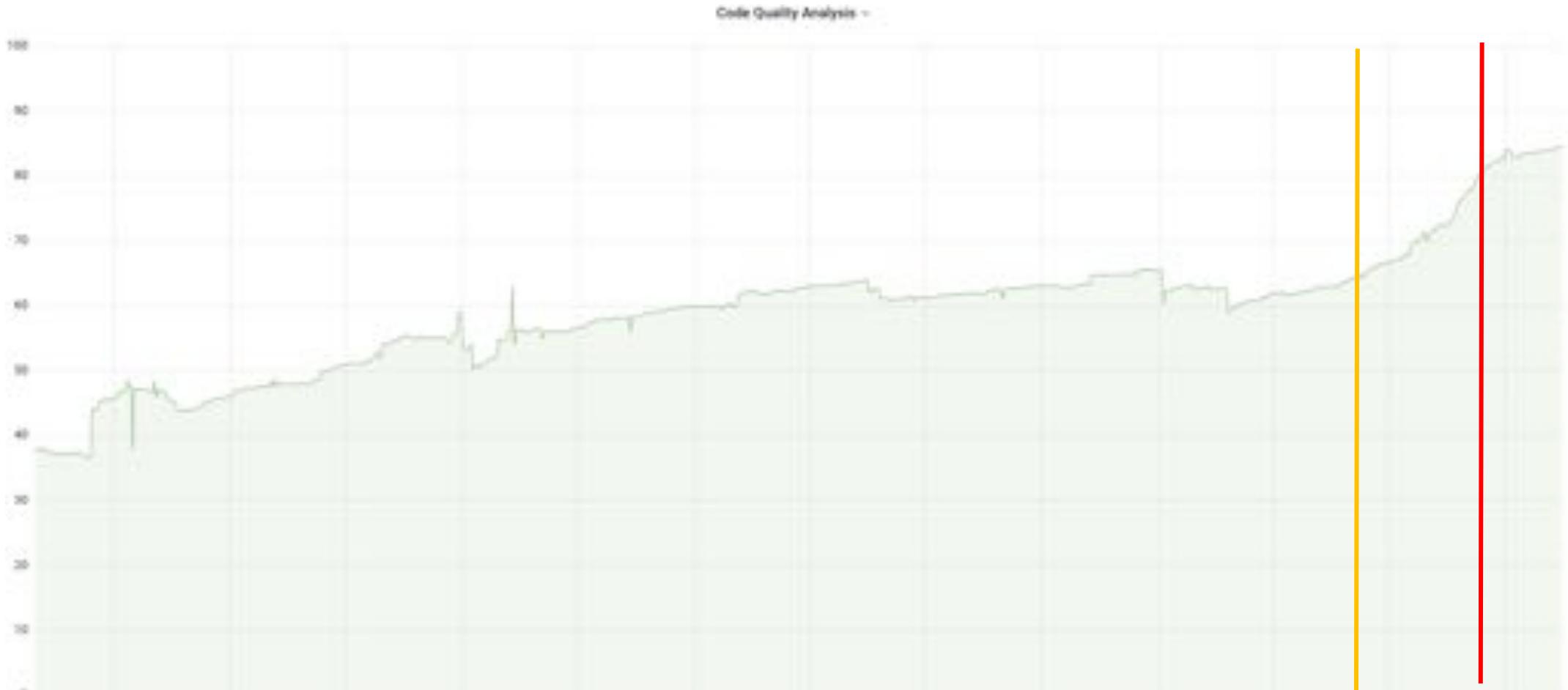
Pipelines Require Code Reviews



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

