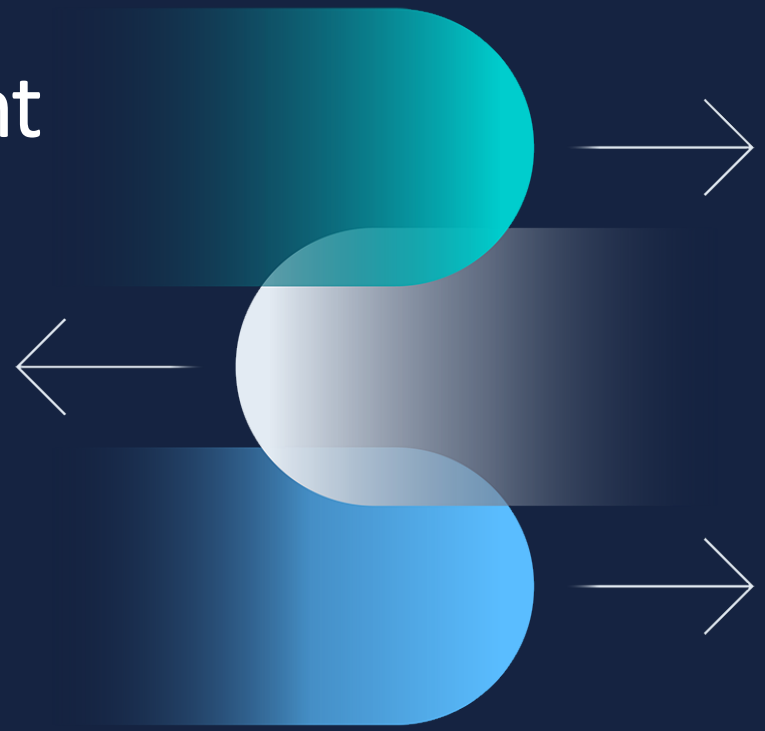
FORM3
FINANCIAL CLOUD

Building our own custom Code Insight tool at Form3

Adelina Simion & Ross McFarlane

Conf42 DevSecOps



Our Customers and Partners

Nationwide Building Society
mastercard
LLOYDS BANKING GROUP
Ebury
paymentsense beyond ordinary
aion
LHV
PPS an Edenred company
Square
ZIGLU
N26

Our People

260 employees

51 nationalities

22 countries

100% remote

Our Investors

$220m in investment so far

Goldman Sachs Asset Management
83NORTH
LLOYDS BANKING GROUP
Nationwide Building Society
mastercard
BARCLAYS
Draper Esprit

Engineering at Form3

FORM3
FINANCIAL CLOUD

Engineering at Form3

Delivering code at scale 🚀

Large number of repos

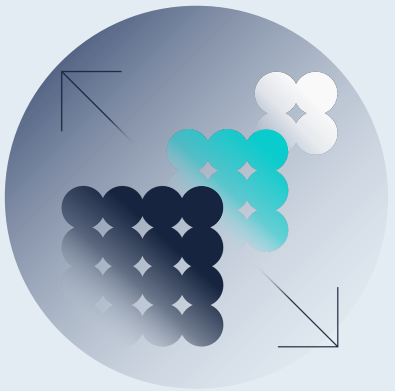
We have over 500 repositories in different languages. Some are not actively maintained, while some are under development

Growing engineering teams

Our teams are in hypergrowth. We have new teams and new engineers contributing to the codebase at rapid pace

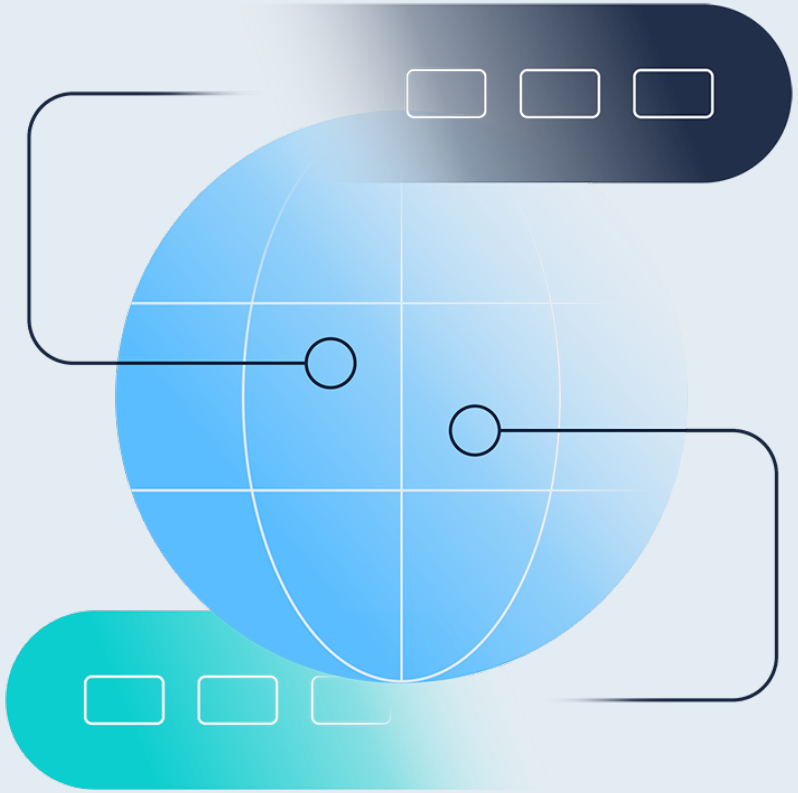
Highest security standards

Our platform is compliant with the highest standards of security. All our repositories should remain free of vulnerabilities



FORM3
FINANCIAL CLOUD

The DevSecOps mindset is crucial at Form3. Our teams own every part of the delivery flow, including the security of their repositories and services



Code analysis at Form3

- Used https://github.com/coinbase/salus for static analysis of our GitHub repos
- Scans ran in one Docker container
- Relatively heavyweight containers of 1GB+

First solution - SecScan

- Our first custom solution to provide standardised scanning across our GitHub repos
- Scans ran in a SecScan docker container
- Tokens for service scanning for each repo
- Teams configured their scans in a Makefile or Travis YAML file on each repository

Problems with SecScan

No enforcement

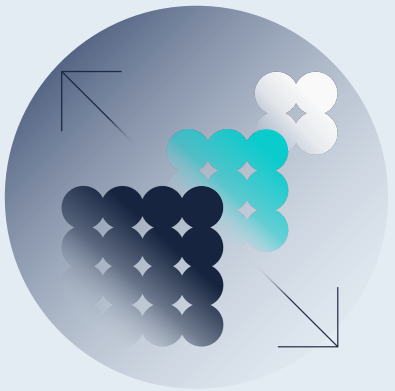
Difficult to enforce rules and code standards across our repositories as setup on new repositories is not mandatory

No visibility

Repositories marking their own homework means attackers could bypass the scan.
Scans run on code commits means possible undetected issues

Lots of maintenance

Initial configuration and maintenance required on each repository when rolling out updates



Code Insight requirements

FORM3
FINANCIAL CLOUD

Code Insight requirements

A better solution was needed! 🚀

The InfoSec team identified some key requirements for a new solution

- Automatic enforcement
- Automatically chosen scans
- Centralised config
- Report on vulnerabilities
- Scan repositories regularly
- Easily build into development pipeline

The Code Insight project was kicked off to implement these requirements and address some of the issues with SecScan 🥳

Teamwork makes the dream work!







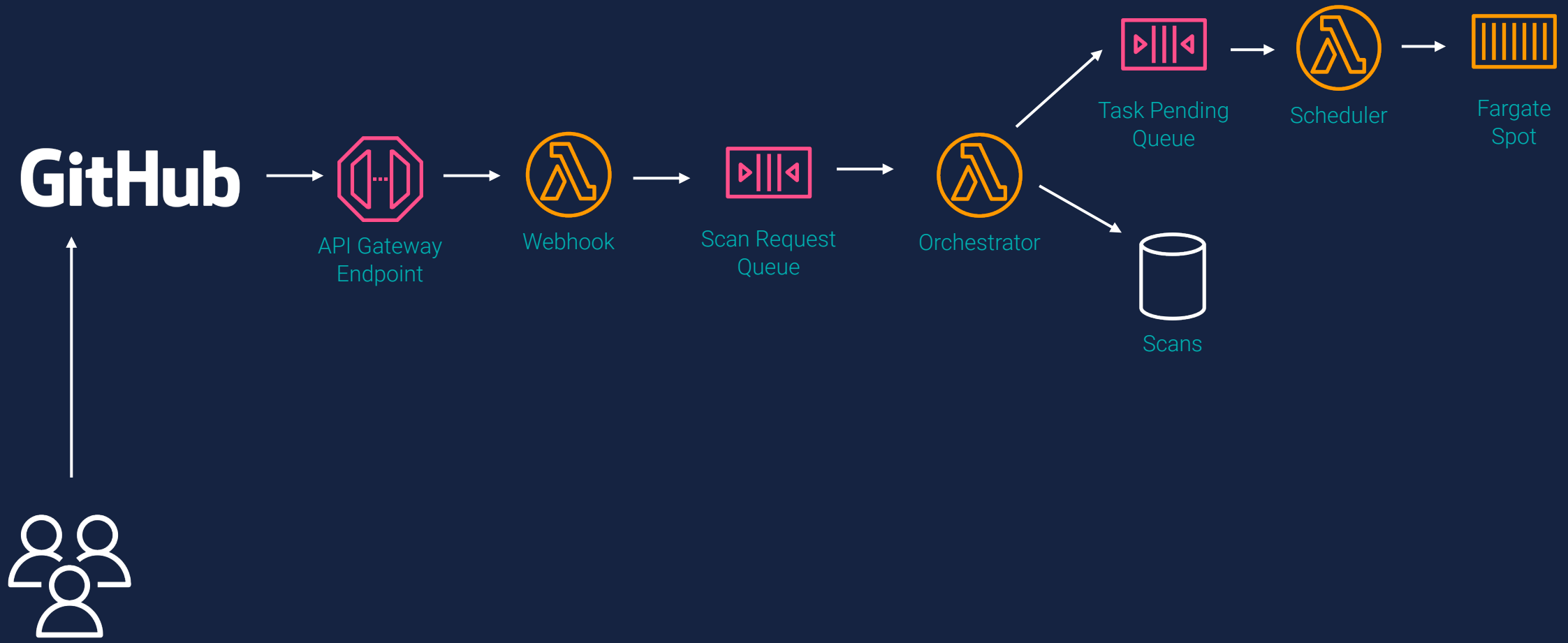




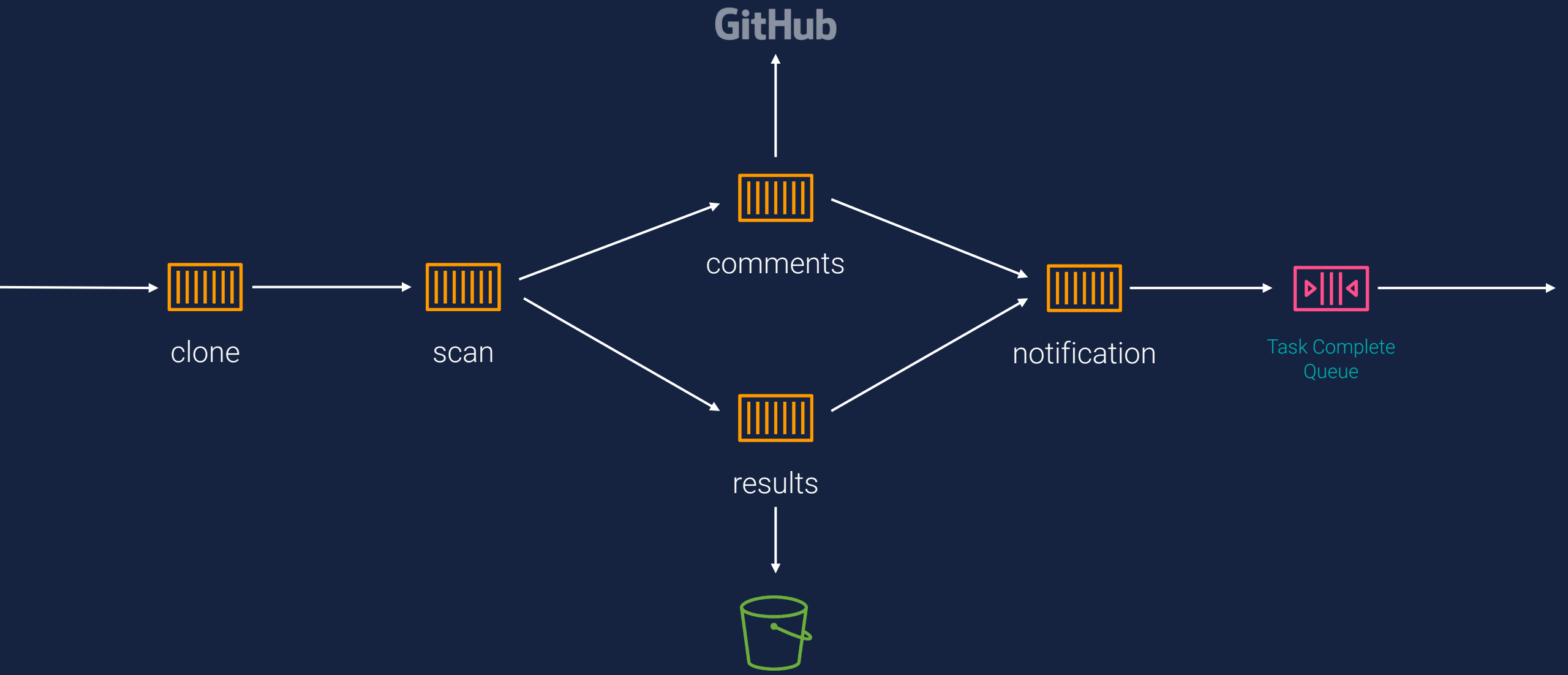
Code Insight architecture

FORM3
FINANCIAL CLOUD

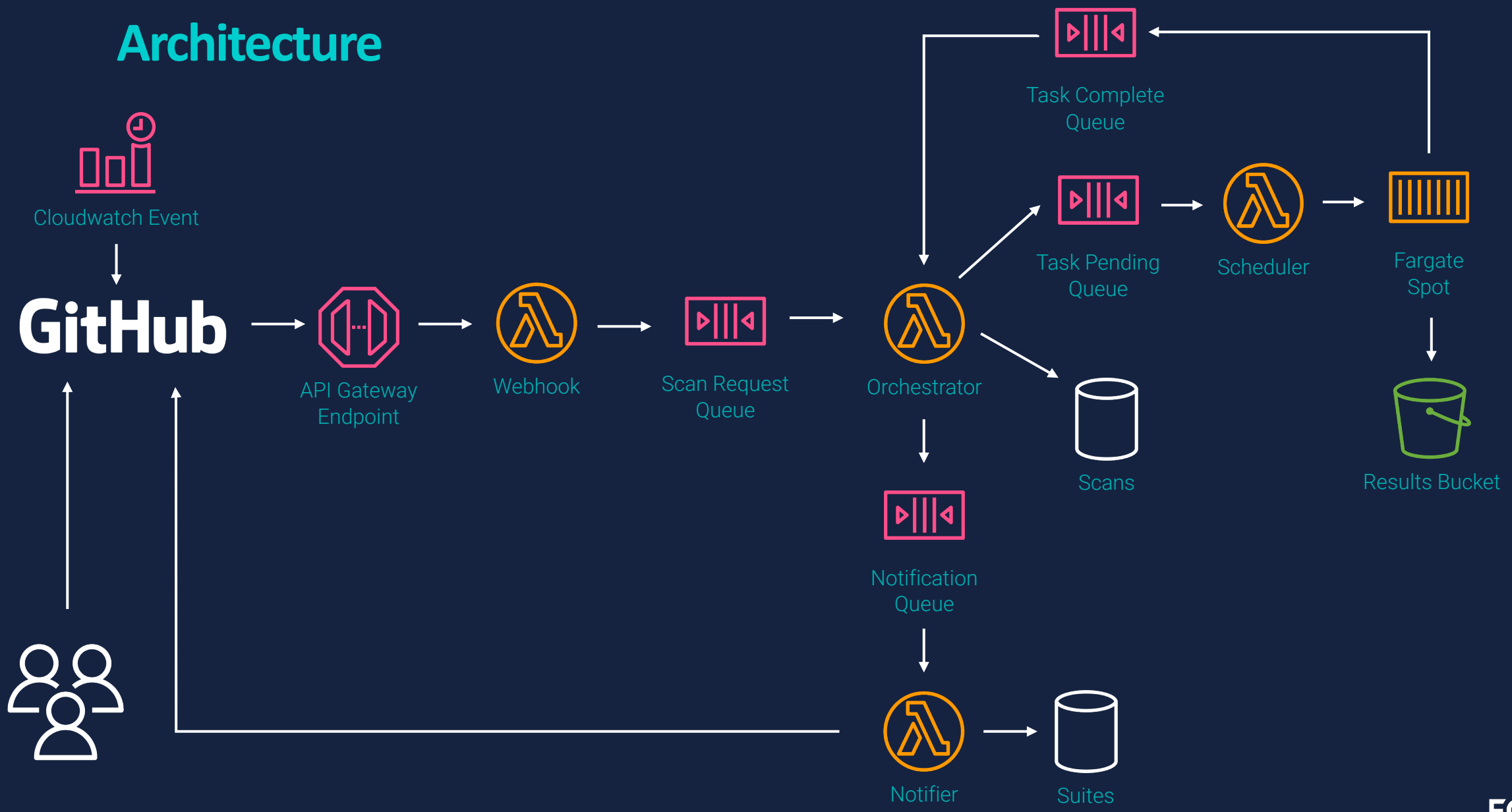
Architecture



Architecture

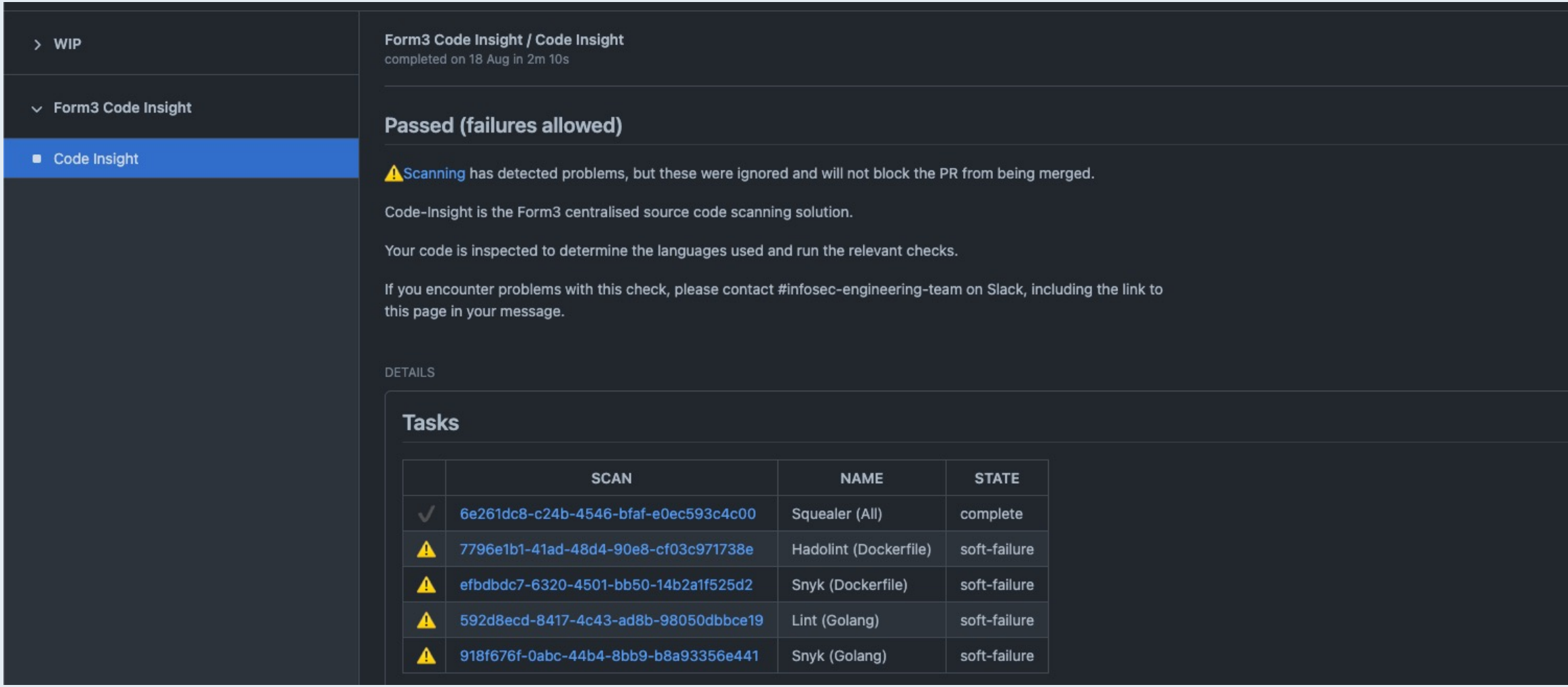


Architecture

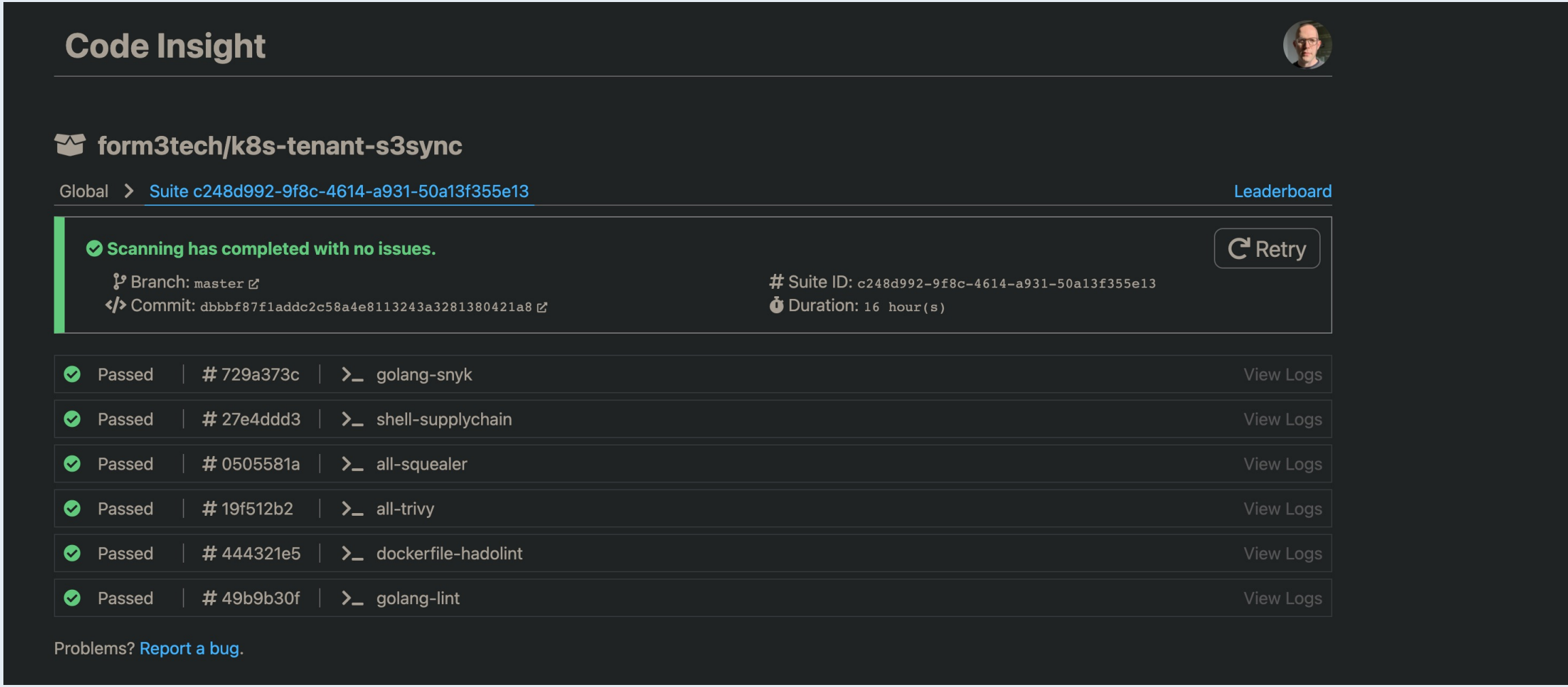


FORM3 FINANCIAL CLOUD

Inspecting your checks 🔎



Inspecting your checks 🔍



Comments on PR

PR comments help our engineers easily identify and fix issues! 🚀

67 postgres/repository.go

Viewed

```
+ func (r *BookingRepo) List(ctx context.Context, hotelID int) ([]innsecure.Booking, error) {
+         stmt := fmt.Sprintf(`select "id", "hotelid", "arrive", "leave", "name" from "Bookings" WHERE hotelid='%d'`, hotelID)
+         rows, err := r.db.Query(stmt)
+         if err != nil {
+                 return nil, fmt.Errorf("failed to list bookings: %w", err)
+         }
+         result := []innsecure.Booking{}
+         for rows.Next() {
+                 var b innsecure.Booking
+                 err = rows.Scan(&b.ID, &b.HotelID, &b.Arrive, &b.Leave, &b.Name)
+                 if err != nil {
+                         fmt.Println(err)
+                         continue
+                 }
+                 result = append(result, b)
+         }
+         return result, nil
+ }
+
+ // ByID returns a single booking by ID.
+ // If no booking is found with the given ID, no error is returned.
+ func (r *BookingRepo) ByID(ctx context.Context, hotelID int, ID string) (*innsecure.Booking, error) {
+         q := fmt.Sprintf(`select "id", "hotelid", "arrive", "leave", "name" from "Bookings" where "hotelid"='%d' AND "id"='%s'`, hotelID, ID)
```

form3-codeinsight on 18 Aug

issue	**gosec**
code	G201
comment	SQL string formatting

Reply...

Resolve conversation

form3-codeinsight on 18 Aug

FORM3 FINANCIAL CLOUD

Benefits

Centralised config makes maintenance a lot easier

New scans are easy to write

☀️ On-demand infrastructure, responds to diurnal pattern of use 🌙

Driving adoption

Introducing Code Insight at Form3

Existing repositories

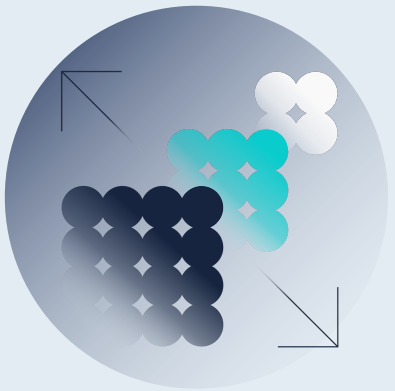
Soft Failures at first, with ‘ratcheting’ approach, and support to raise coverage

New Repositories

Automatically enforced for all new repositories

Metrics

We gather metrics from scan results to help us assess vulnerabilities and Code Insight’s performance



FORM3
FINANCIAL CLOUD

Driving Adoption

Batch PRs

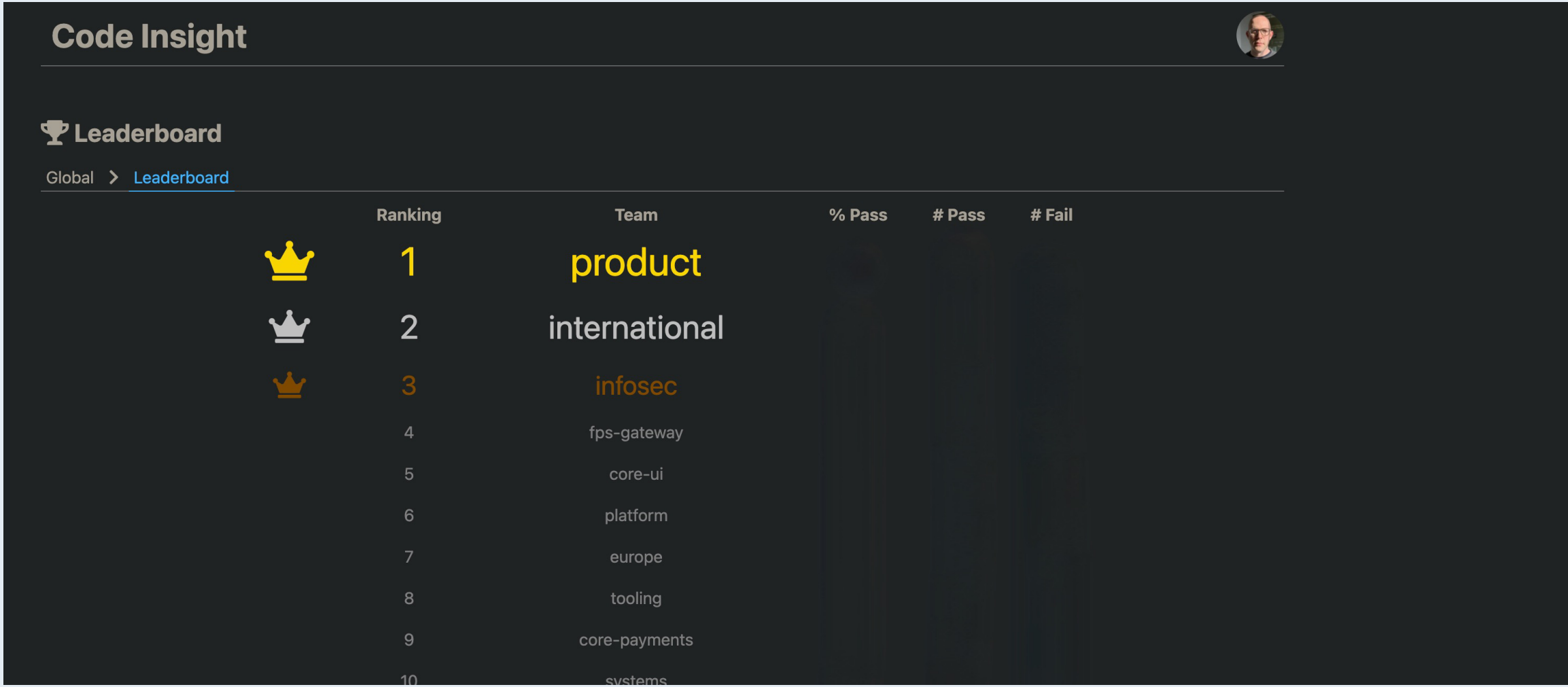
Mob sessions

to improve coverage

Some gamification with

Team Leaderboard

Gamification



Insights from Code Insight

FORM3
FINANCIAL CLOUD

Stuff that didn’t go so well

A flaky scan can put the brakes on the engineering team

Large repositories are tricky to reform

New vulnerabilities can break a build when you least expect it

Upcoming features/improvements

Work in progress

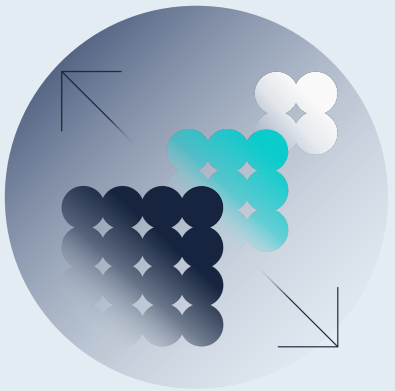
We want to improve our detection to distinguish between old and newly introduced errors

Insight metrics monitoring

We have more work to do on the monitoring of Code Insight metrics

Policy adjustments

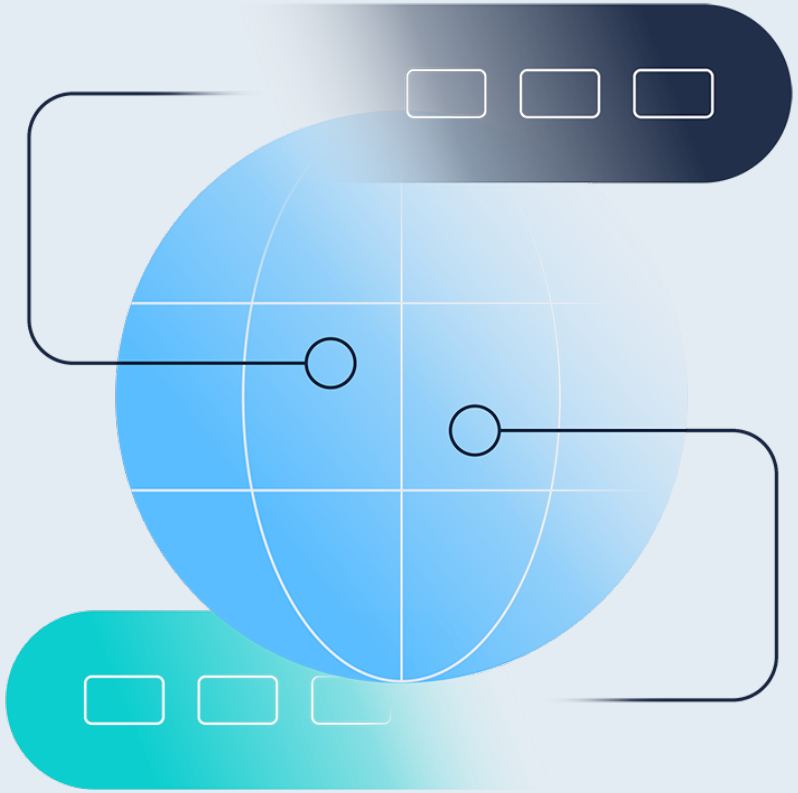
We have found Code Insight to be too sensitive to failures at times. We should incorporate our policies of age & severity in the failures.



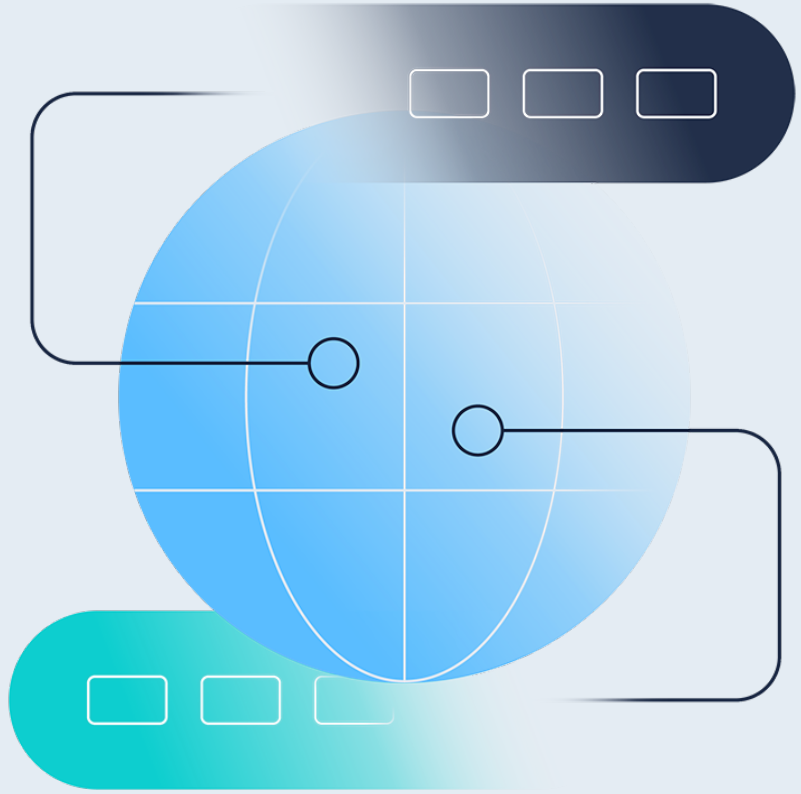
Conclusions

FORM3
FINANCIAL CLOUD

Code Insight allowed Form3 to streamline development work.

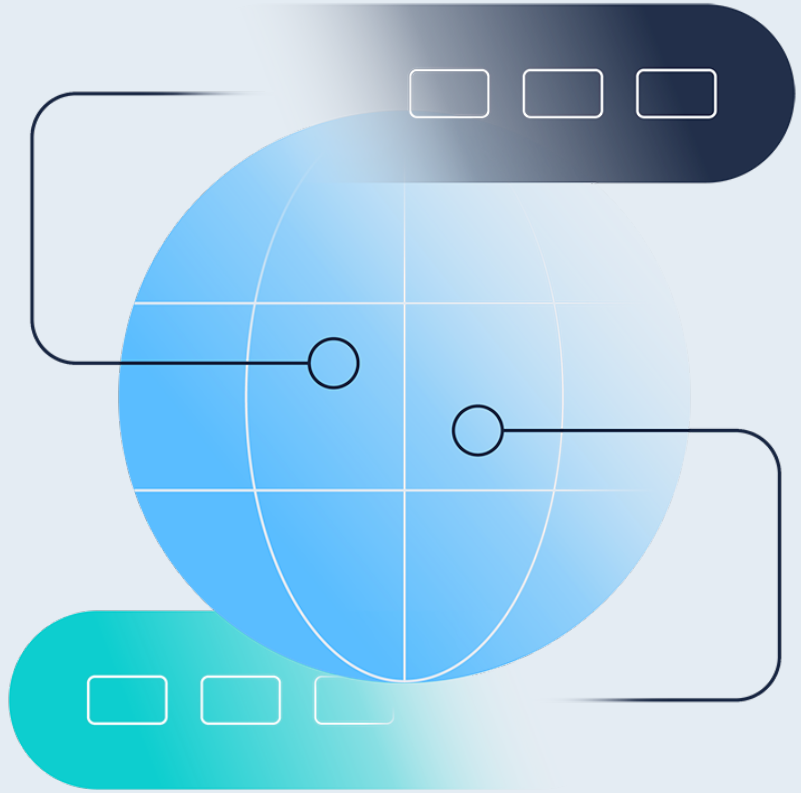


Nightly builds, alongside PR builds, ensure that we have an up-to-date view of our vulnerabilities.

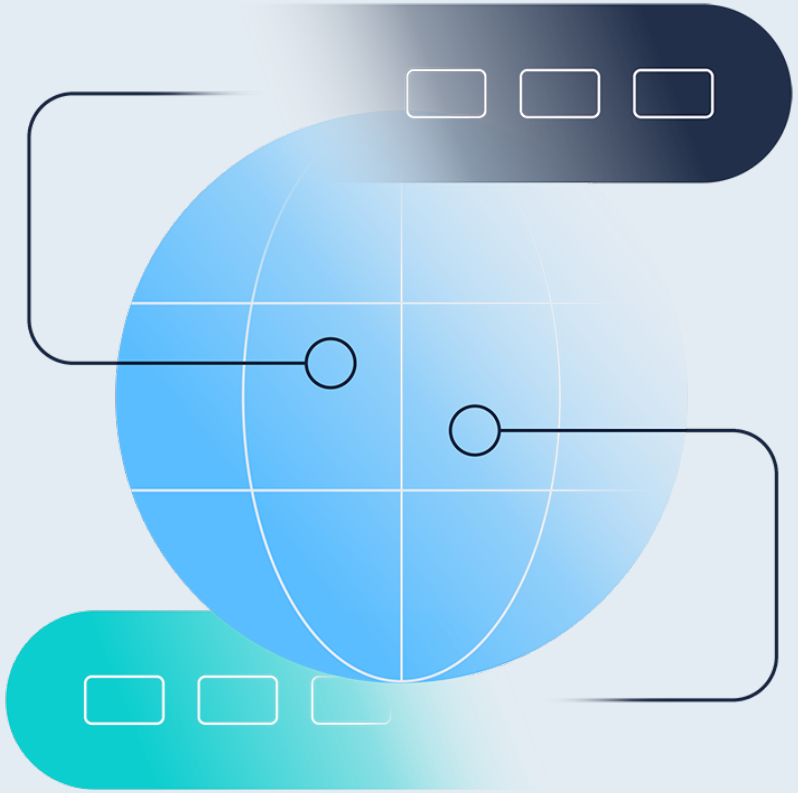


GitHub integration and PR comments were helpful for our engineers to fix issues.

Gamification was not meaningful to this project.



No extra config and easy maintenance were big improvements to our previous code scanning solution.



Thanks for listening! 🎤👊⬇️

Adelina Simion

addetz

classic_addetz

Ross McFarlane

rossmcf

rossmcf

Check out our careers site, podcast and our engineering site!

form3.tech/careers

techpodcast.form3.tech

engineering.form3.tech