DevOps Conference 2024

Fortify your DevOps security

Lorenzo Barbieri

lorenzo.barbieri@softwareone.com

DevOps Conference

Microsoft avanade eng software one BC Soft KRATEO PLATFORMOPS UNIKEY blexin CON NOI È SEMPLICE

SPONSOR


Microsoft


avanade


eng


software
one


BC Soft
consulenza sistemi informativi


blexin
CON NOI È SEMPLICE


KRATEO
PLATFORMOPS


UNIKEY

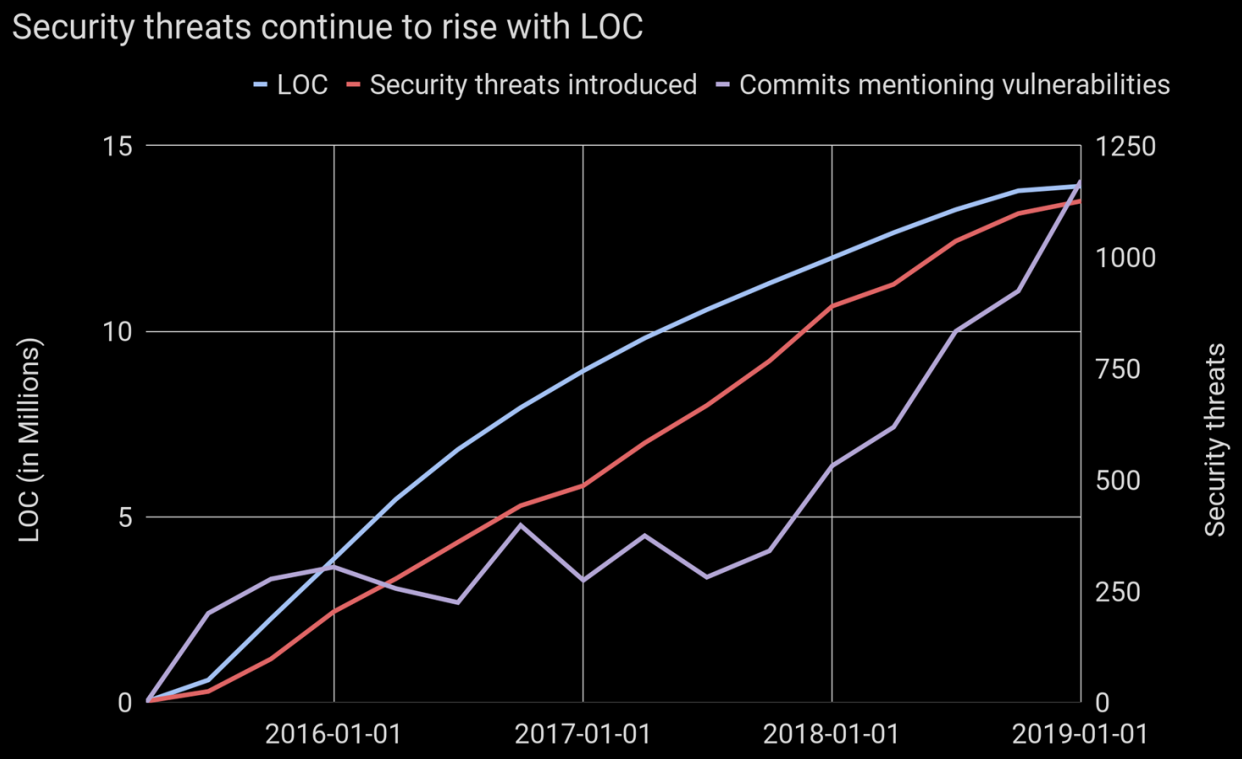

Packt


JET
BRAINS


NET
CODE

Why DevOps Security?

More code = more technical debt & exposure

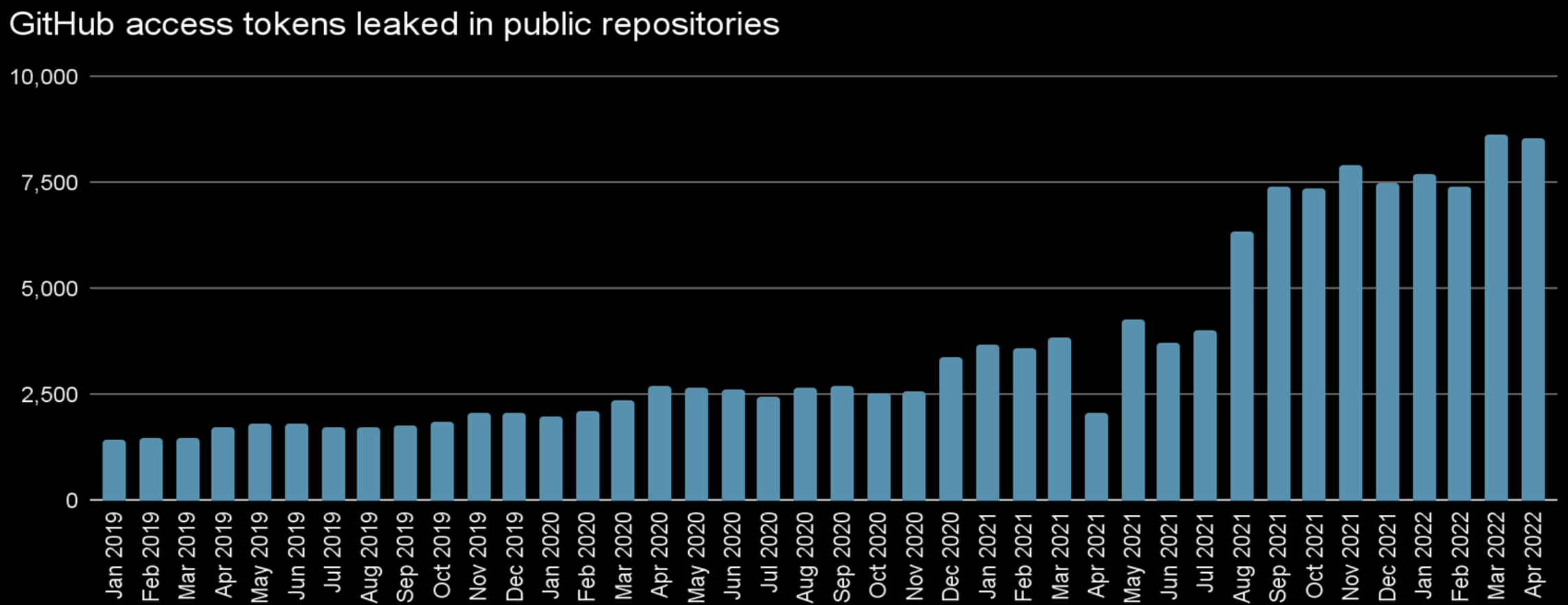


Flaws in applications are consistently the #1 attack vector for breaches

Source: GitHub Data Science Team analysis of 70 million lines of code in major OSS projects added over a 5 year period

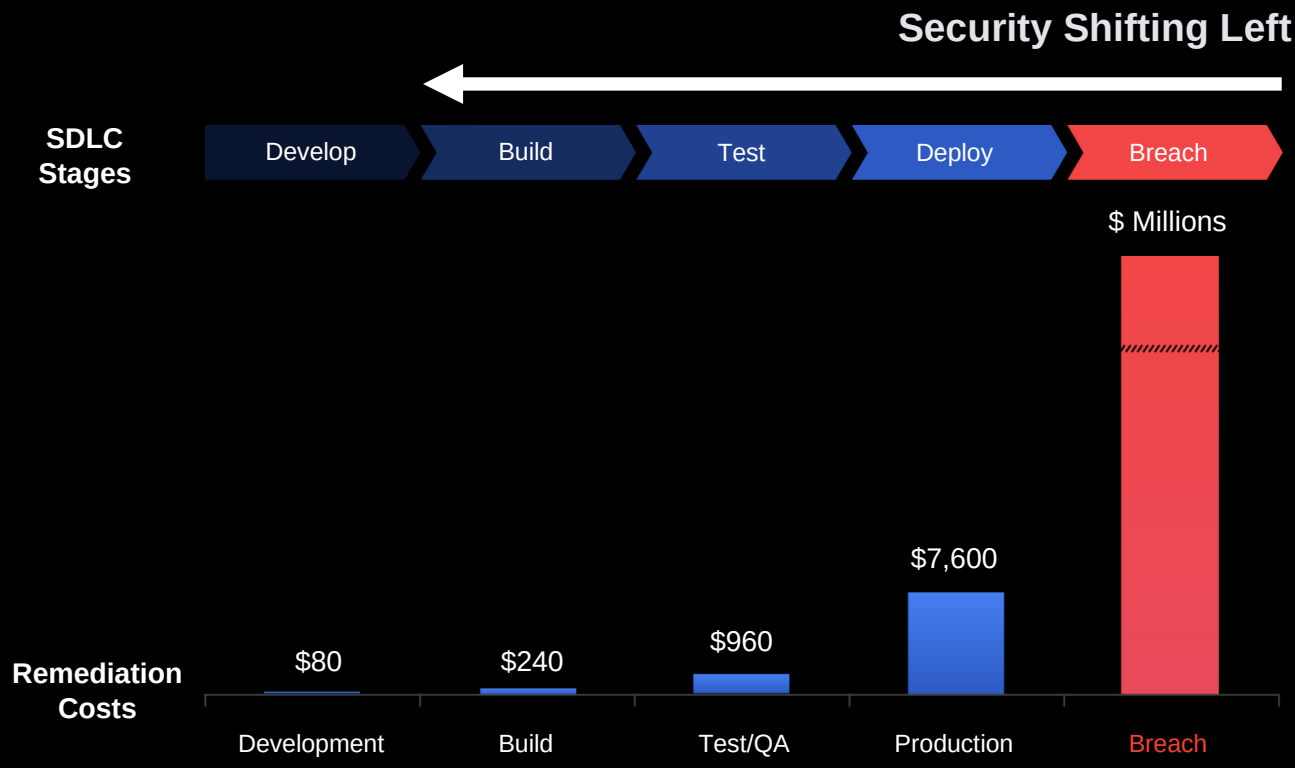
Source: Verizon Data Breach Investigations reports 2016, 2017, 2018, 2019 and 2020.

We’re seeing more credential leaks than ever

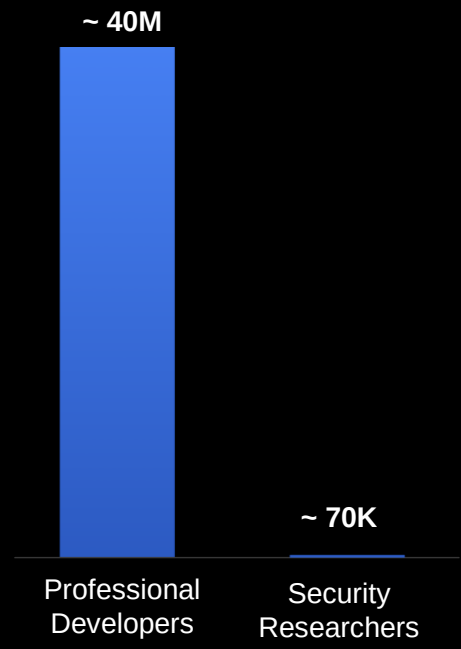


Source: GitHub data

Shifting security left, but why?

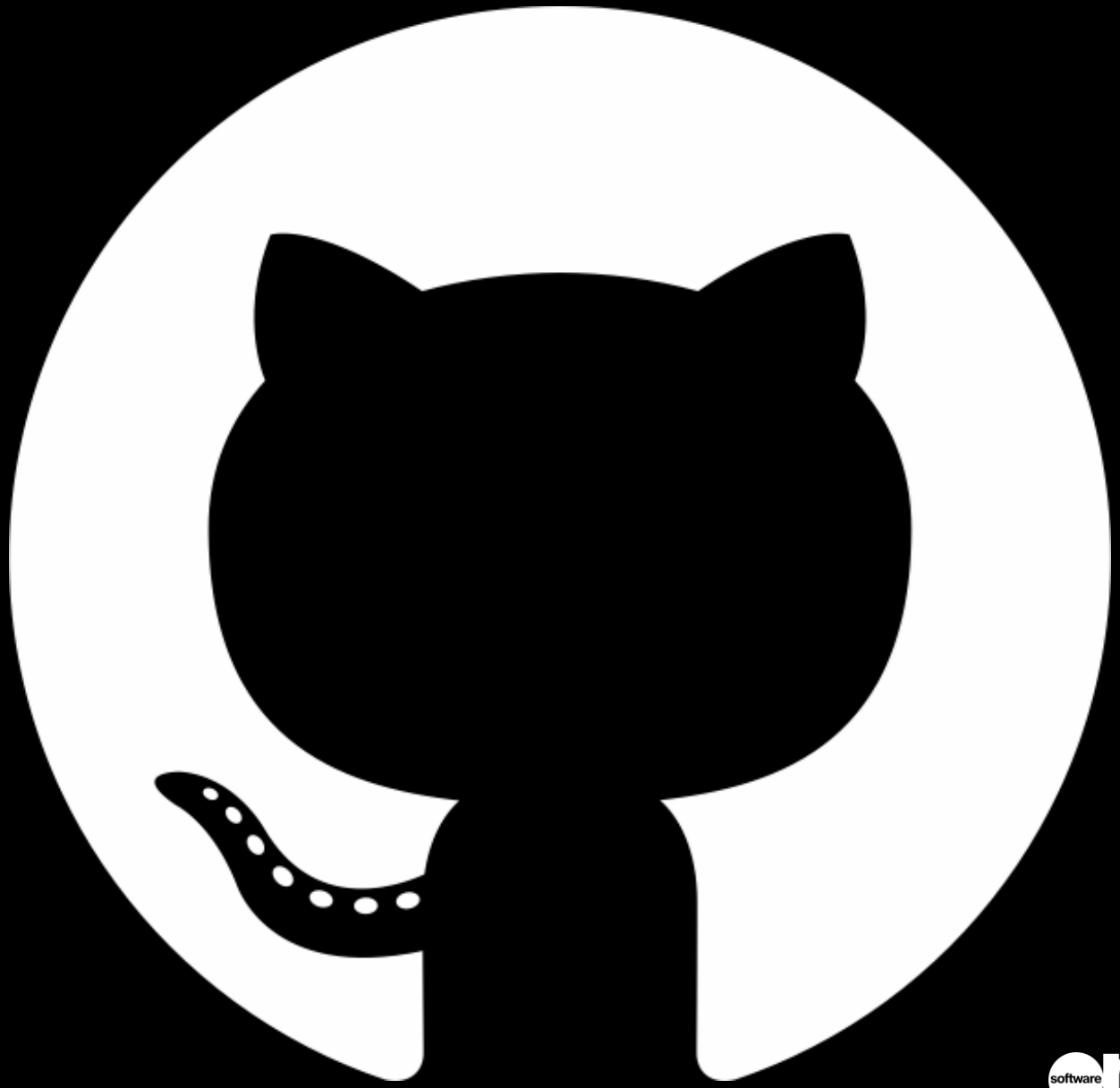


Vastly more cost effective to remediate during development



570x more developers than security researchers

GitHub Advanced Security



GitHub’s Advanced Security Capabilities

	Public repository	Private repository without Advanced Security	Private repository with Advanced Security
Code scanning	✓	✗	✓
CodeQL CLI	✓	✗	✓
Secret scanning	✓	✗	✓
Custom auto-triage rules	✓	✗	✓
Dependency review	✓	✗	✓

The Engine - CodeQL

Analyze code as data using expressive queries to say what you want to find, not how to find it

Quickly refine analyses to increase precision within your codebase

Share security knowledge within your teams using codified, readable and executable queries

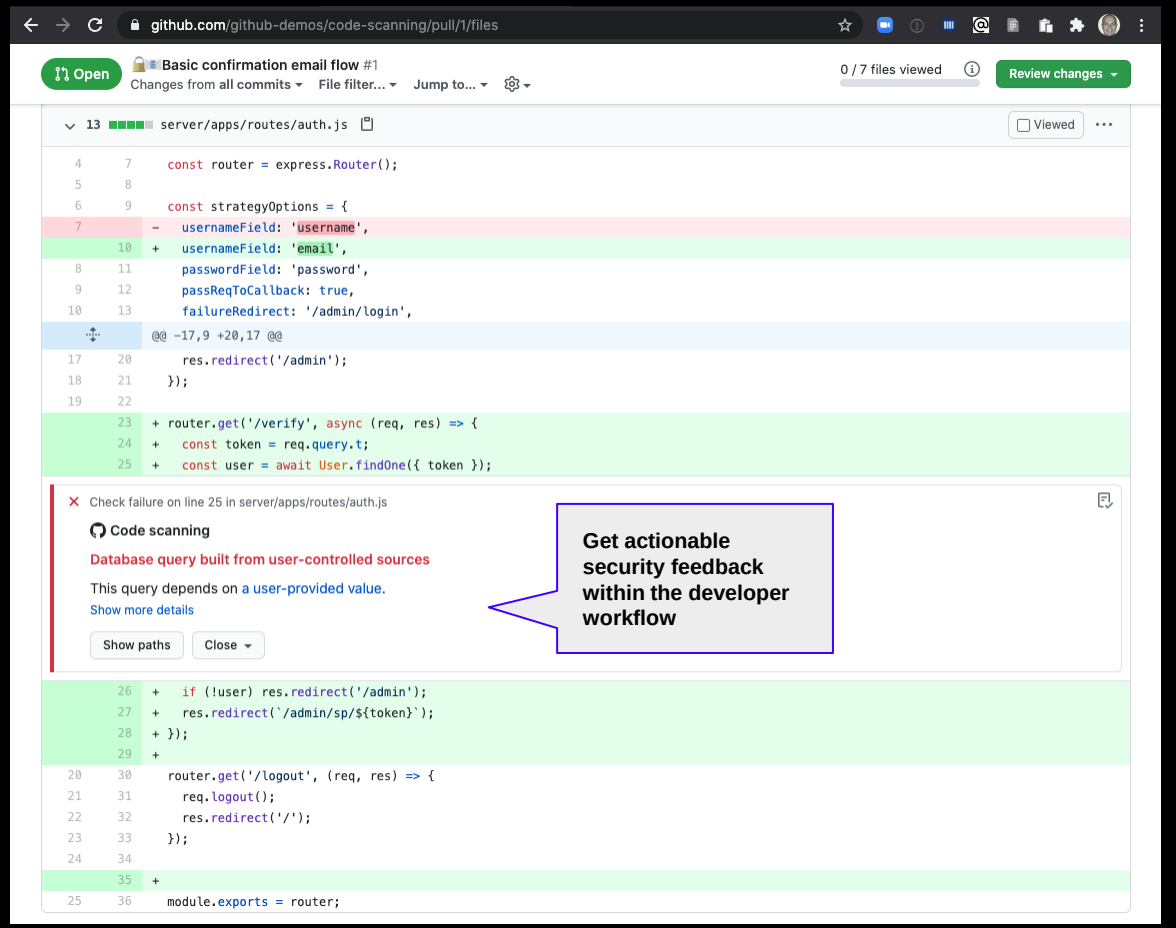
Secure your source code

Find and fix vulnerabilities as code is developed

- Deep Semantic Analysis
- Native to the developer experience
- Prevent vulnerabilities merging into main

Customize queries and leverage community

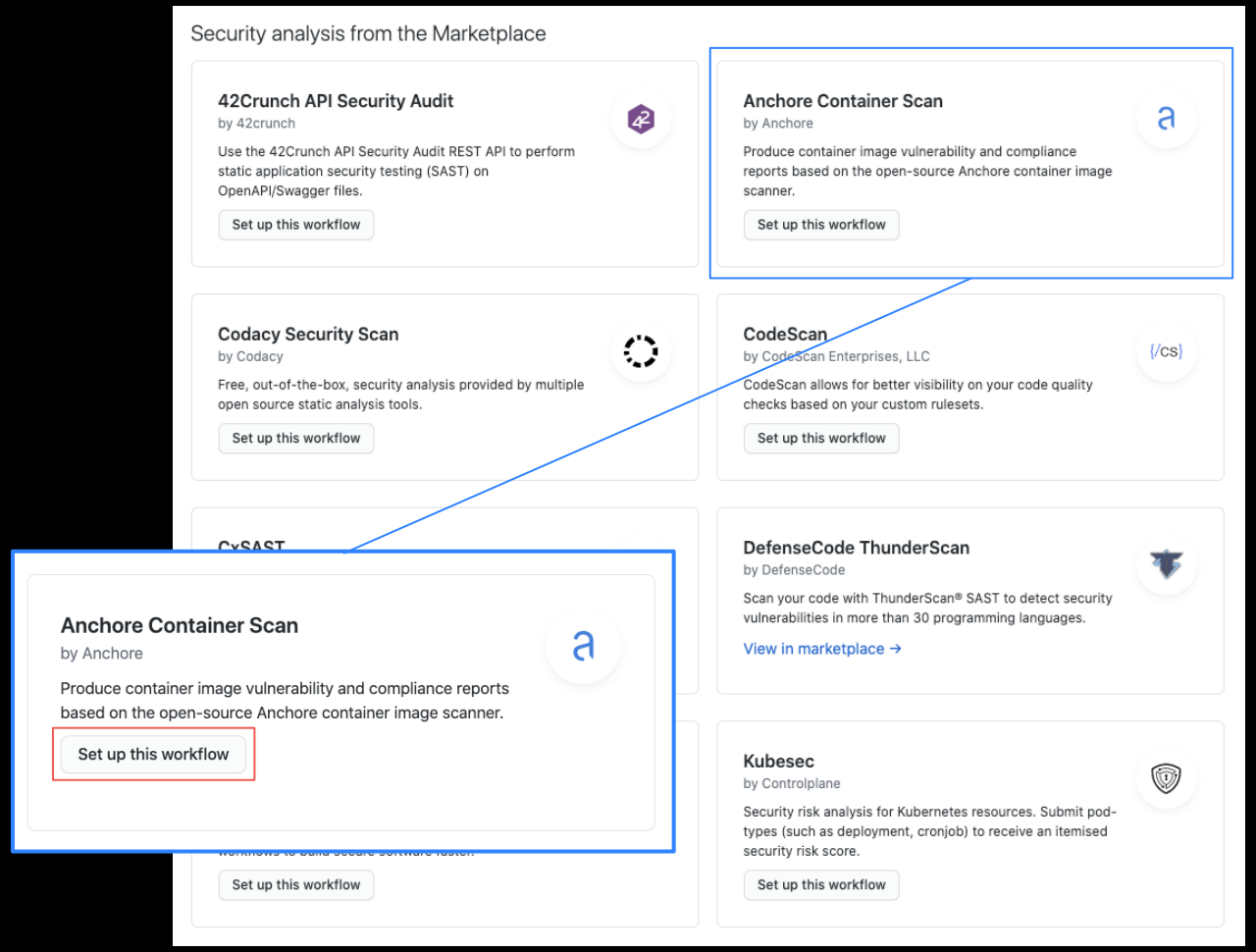
- Community of researchers collaborating
- Partner to respond to 0-days



Ecosystem of Security tools

Power your security with an Ecosystem

- Single tools don’t solve all security problems
- Platform for unification of Security tools
- Continuously growing ecosystem



Combining CodeQL with the world's largest developer community gives next generation SAST performance

(Software Application Security Testing)

20,000

public repos have enabled automated code review using CodeQL (before it's native!)

1,700+

open source queries with contributions from Microsoft, Google and many others

72%

fix rate for potential vulnerabilities flagged in open source projects

35%

of recent JS CVEs would have been identified by a default CodeQL query

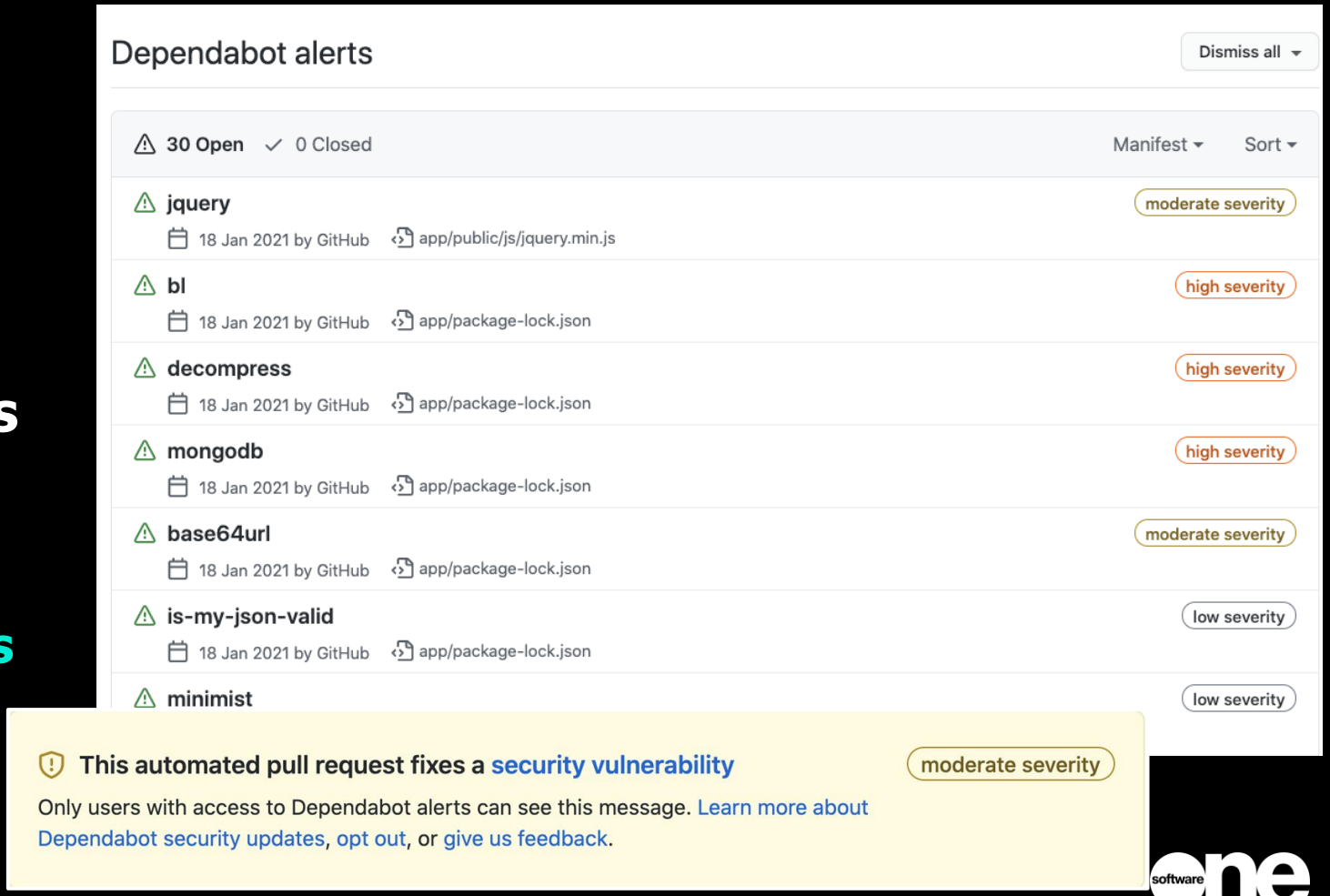
Secure your supply chain

Know your environment

- Dependency Graph
- Dependency Insights

Manage your dependencies

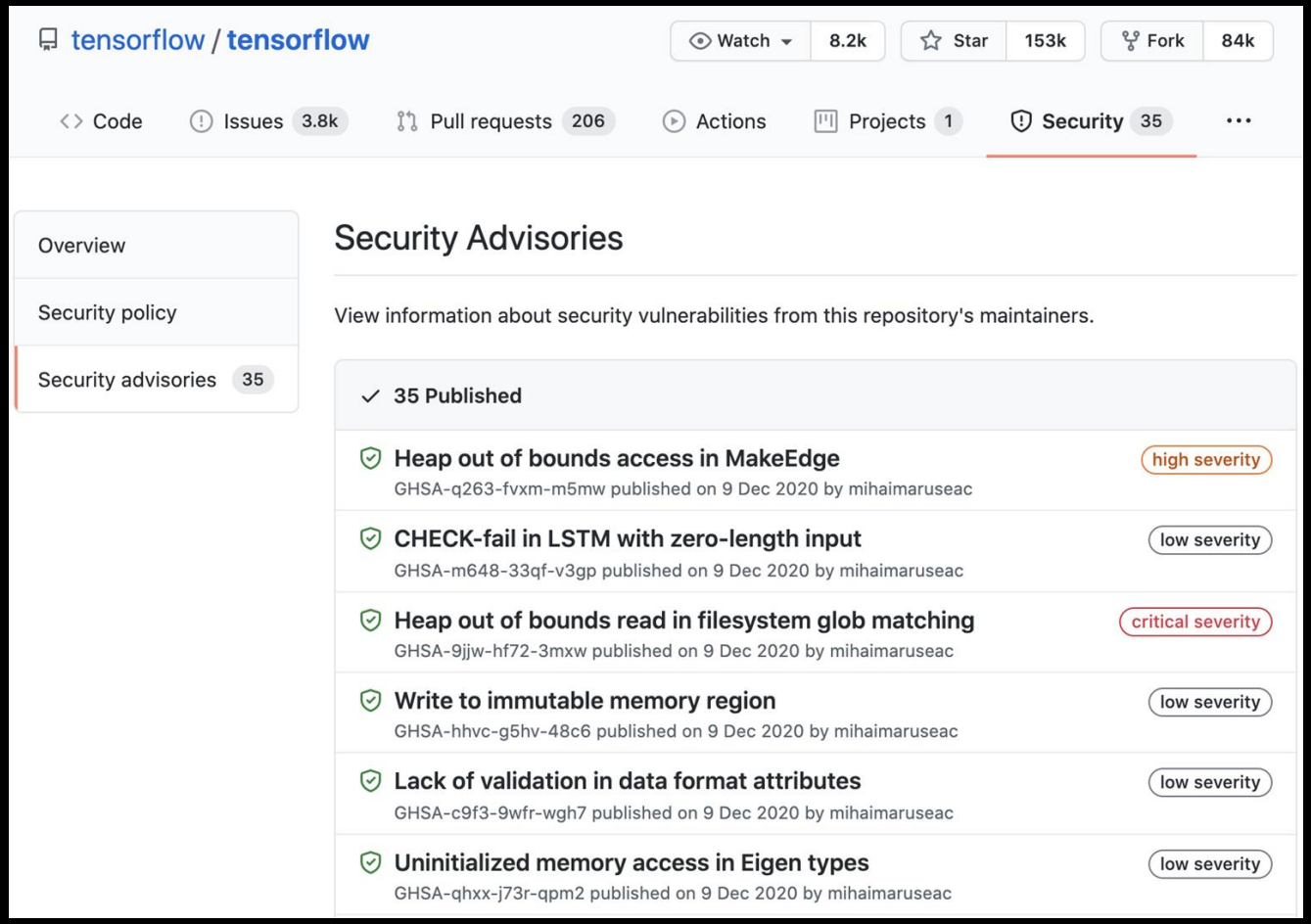
- Dependabot alerts
- Dependabot security updates
- Dependabot version updates



Secure your supply chain

Fix and publish vulnerability information

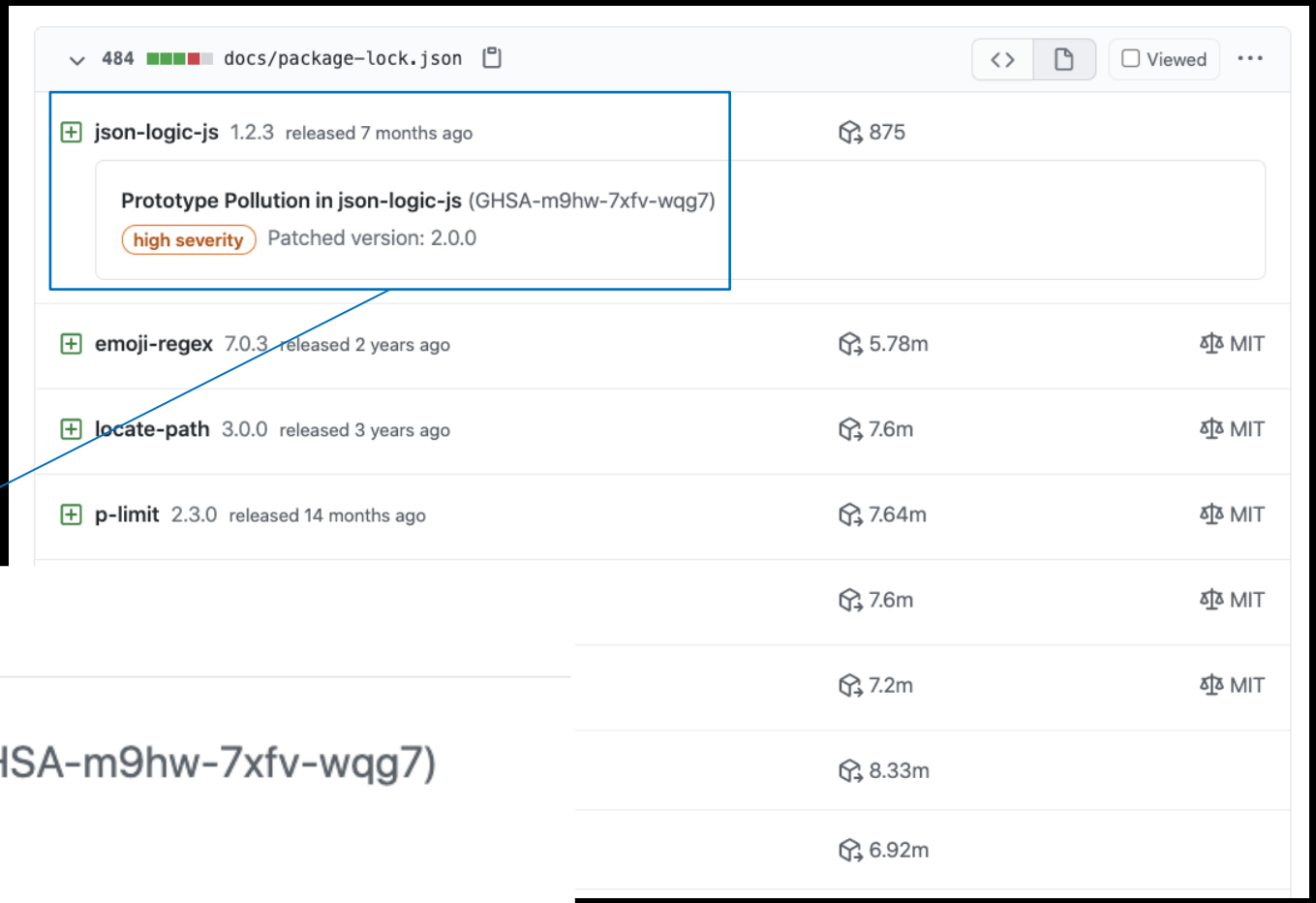
- **SECURITY.md**
- **Security Advisories**
- **GitHub Advisory Database**

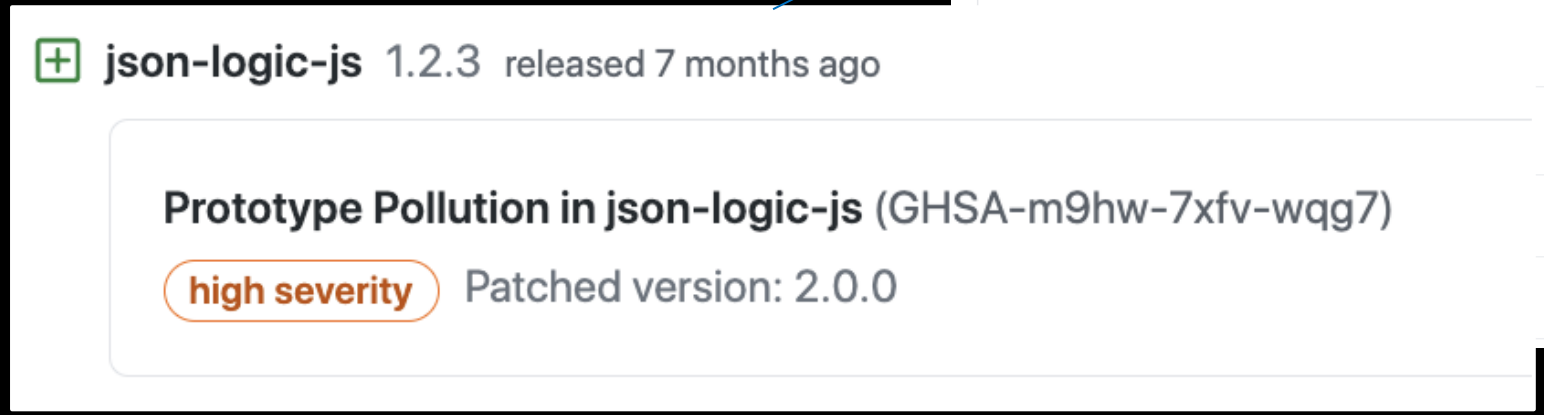


Secure your supply chain

Dependency Review

- Review Dependency
- Feedback in Pull Request
- Dependency Licensing

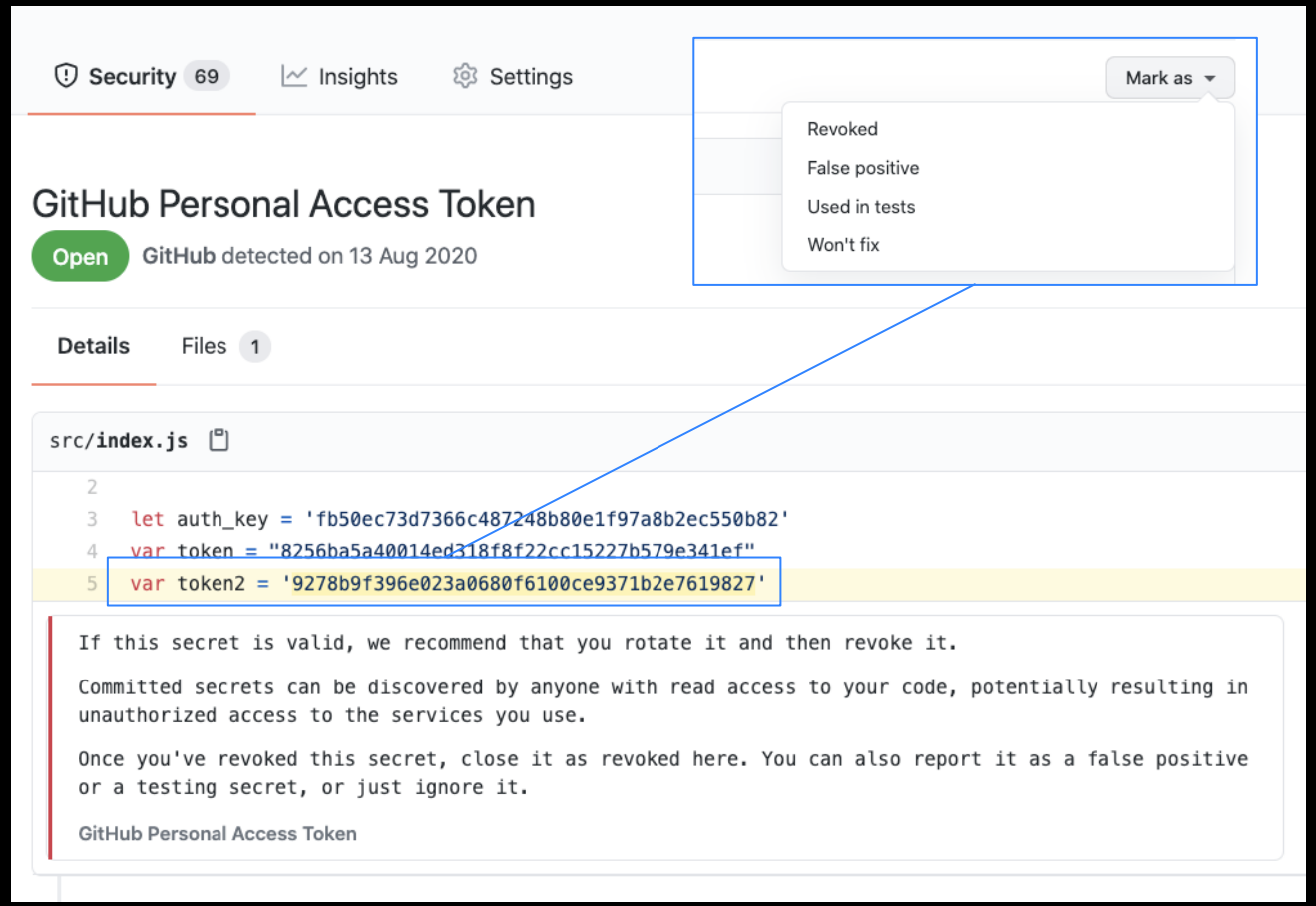




Secure your secrets

Find hard-coded secrets in code base

- Discover published secrets
- Git history and branch analysis
- Proactive prevent secrets from being leaked
- Continuous development with cloud partners




adafruit

Alibaba Cloud

aws

ATLASSIAN

Azure

CloudBees
CodeShip

databricks

DISCORD

Dropbox

GOCARDLESS

Google Cloud

HubSpot

HashiCorp

@mailgun

npm

Palantir

POSTMAN

proctorio

pulumi

samsara

slack

stripe

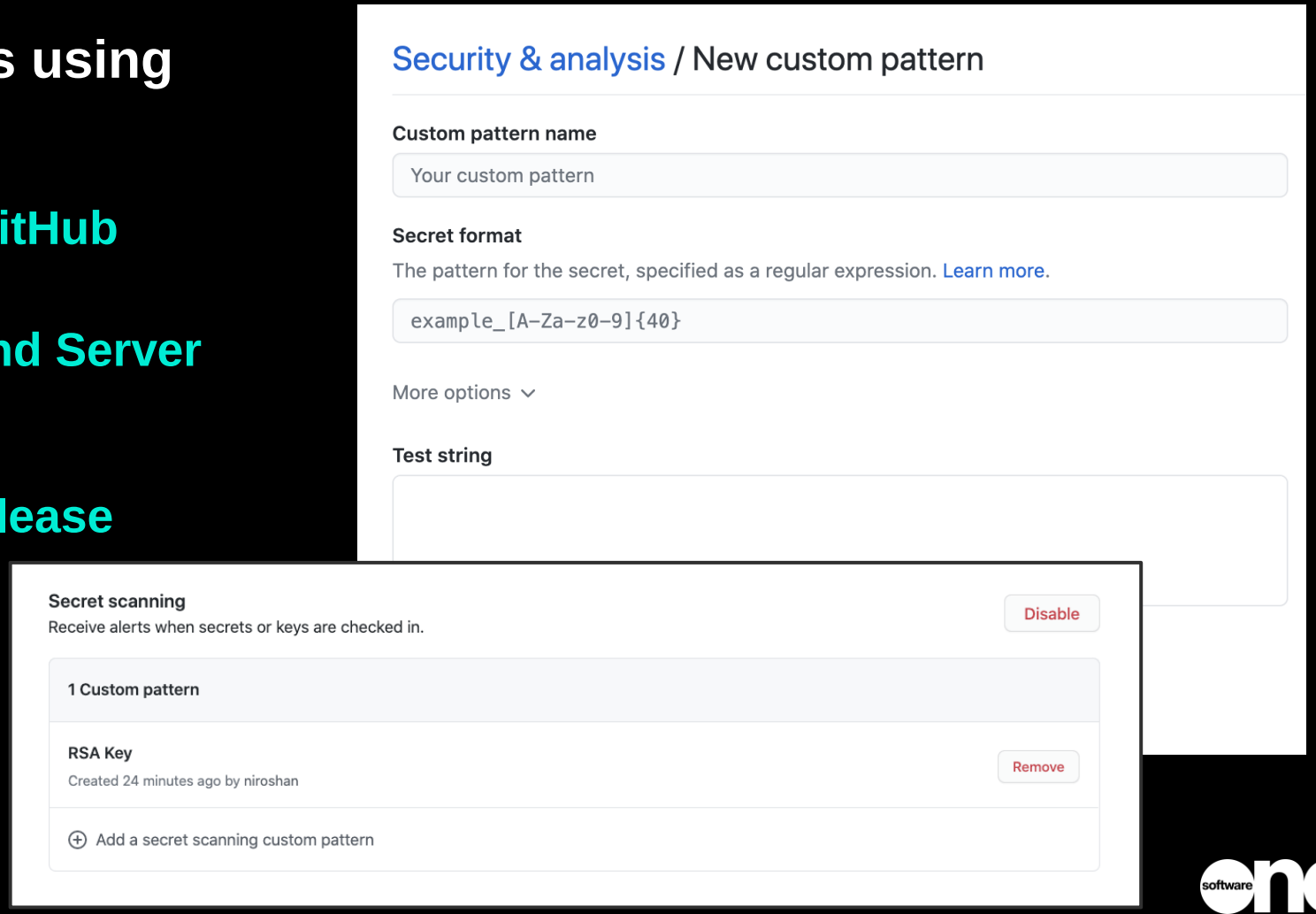
Tencent 腾讯

And more...

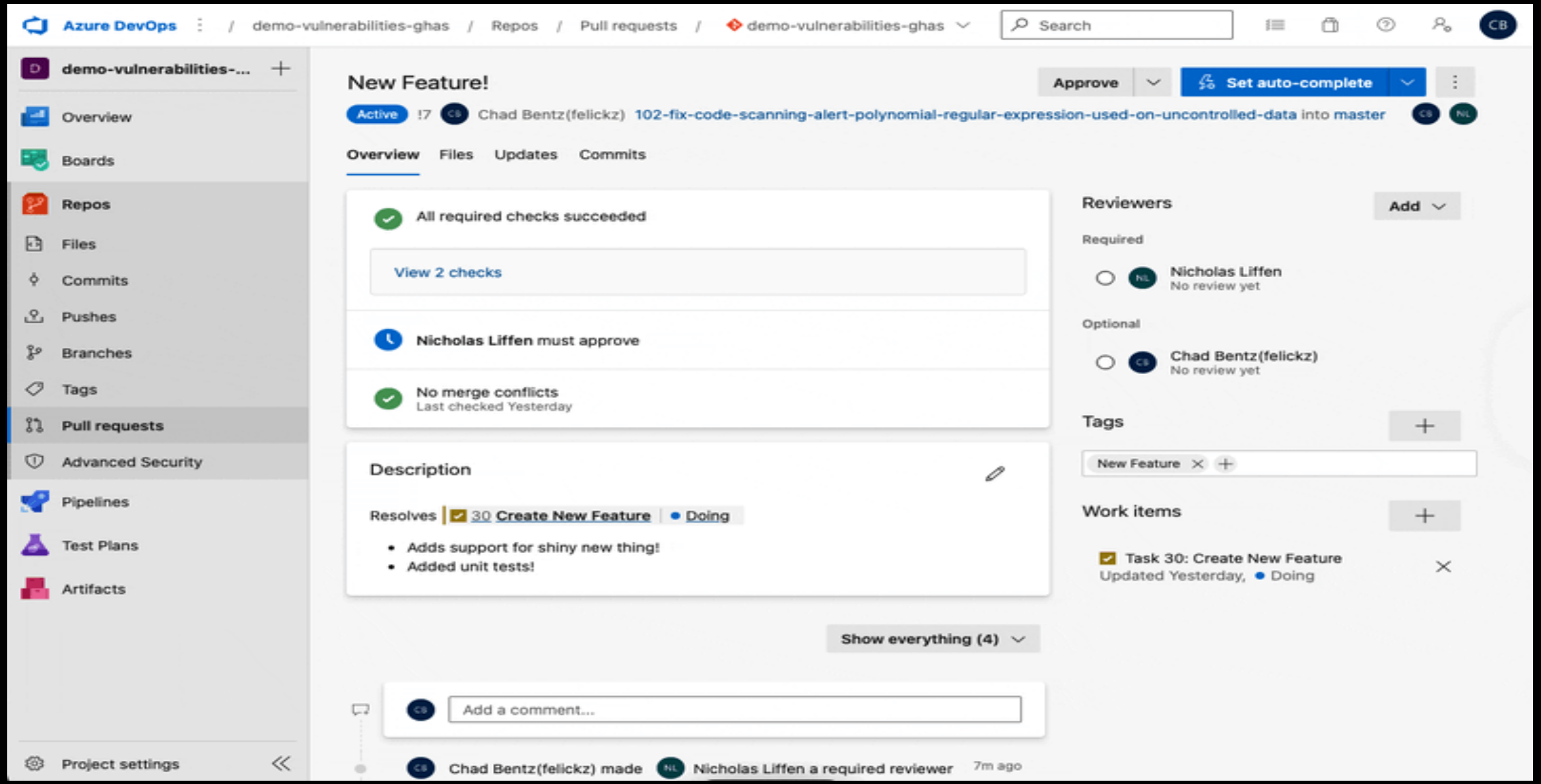
Secure your secrets

Find your custom secrets using custom patterns

- Define custom patterns in GitHub
- Repository, Organisation, and Server Instance based patterns
- Test your patterns before release

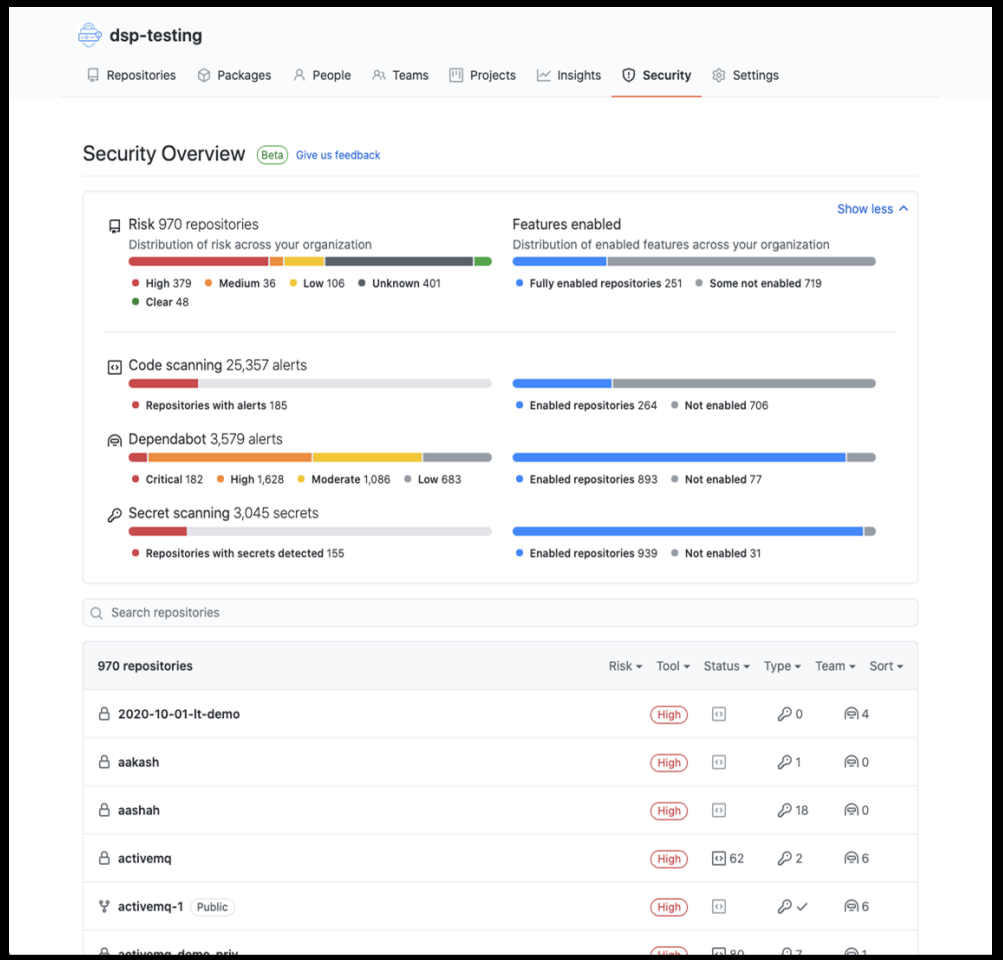


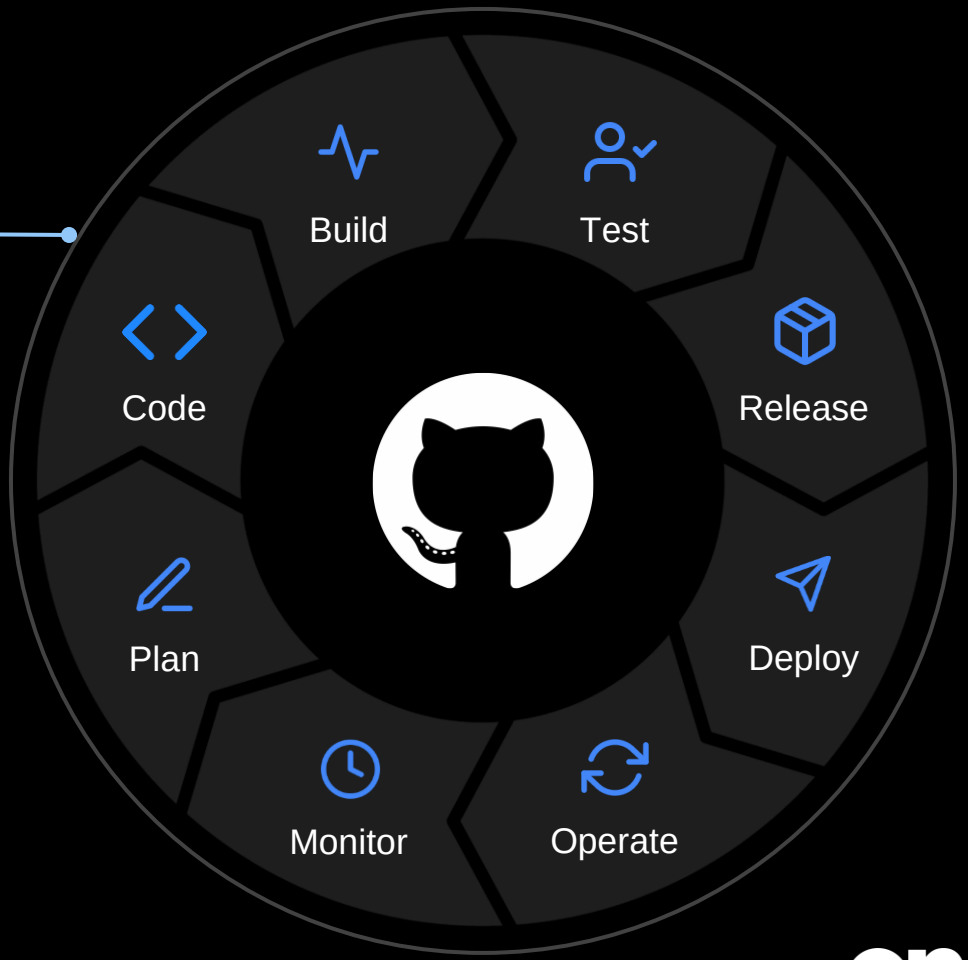
GitHub Advanced Security is available also for Azure DevOps


Azure DevOps / demo-vulnerabilities-ghas / Repos / Pull requests / demo-vulnerabilities-ghas
Search
CB
demo-vulnerabilities-...
Overview
Boards
Repos
Files
Commits
Pushes
Branches
Tags
Pull requests
Advanced Security
Pipelines
Test Plans
Artifacts
Project settings
New Feature!
Approve
Set auto-complete
Active !7 Chad Bentz(felickz) 102-fix-code-scanning-alert-polynomial-regular-expression-used-on-uncontrolled-data into master
Overview Files Updates Commits
All required checks succeeded
View 2 checks
Nicholas Liffen must approve
No merge conflicts
Last checked Yesterday
Description
Resolves 30 Create New Feature Doing
Adds support for shiny new thing!
Added unit tests!
Reviewers
Add
Required
Nicholas Liffen
No review yet
Optional
Chad Bentz(felickz)
No review yet
Tags
New Feature
Work items
Task 30: Create New Feature
Updated Yesterday, Doing
Show everything (4)
Add a comment...
Chad Bentz(felickz) made Nicholas Liffen a required reviewer 7m ago

Security Built into the Developer LifeCycle

Organisation wide view





40 days

Mean time to remediate (MTTR)

for repos with Dependabot security updates

180+ days

Mean time to remediate (MTTR)
Industry norm

Do you really believe Ops people use GitHub?

What about Defender for Cloud?

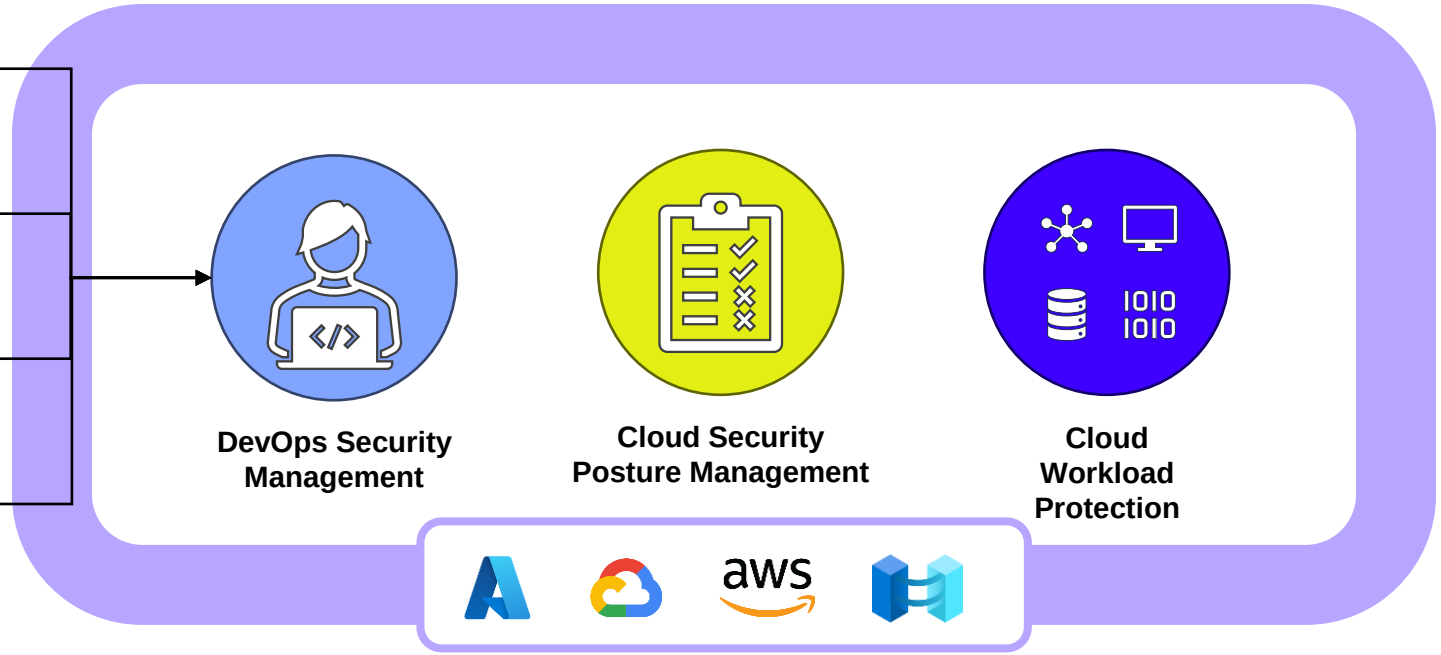
It supports DevOps environments!

DevOps posture visibility
Code|Dependences|Secrets|Container images|IaC insights

Infrastructure as code security
ARM|Bicep|Terraform|CloudFormation|and more

Code to cloud contextualization
Across multipipeline and multicloud environments

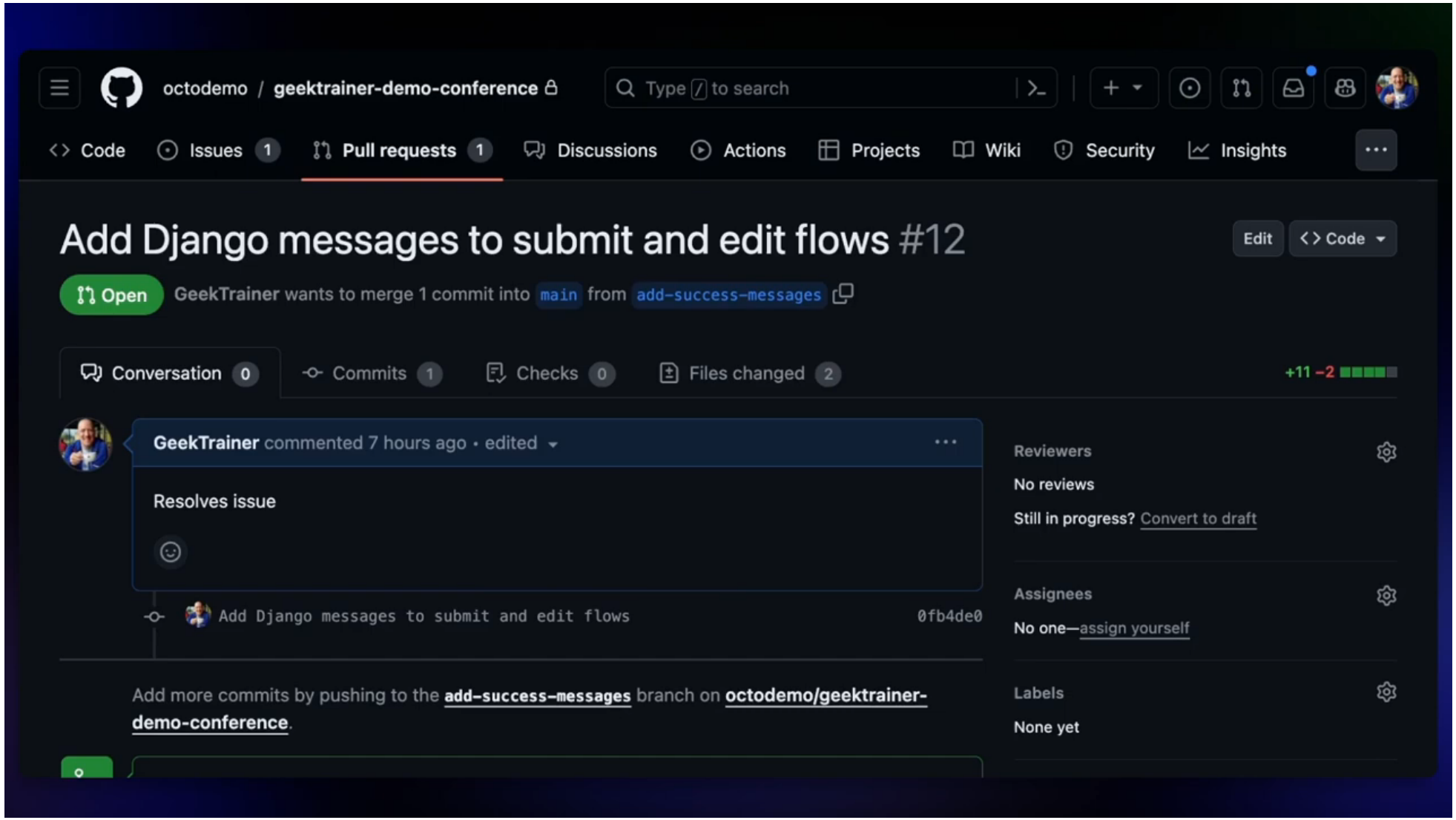
Integrated workflows
Pull request annotations|Developer ownership assignments



GitHub Copilot

You can’t do a session in 2024 without talking about Copilots!

GitHub Copilot Enterprise – PR Review



Thank you and...

Vota Lorenzo!

lorenzo.barbieri@
softwareone.com