

DevOps Conference 2024

Fortify your DevOps security



Lorenzo Barbieri

lorenzo.barbieri@softwareone.com



DevOps

Conference



SPONSOR

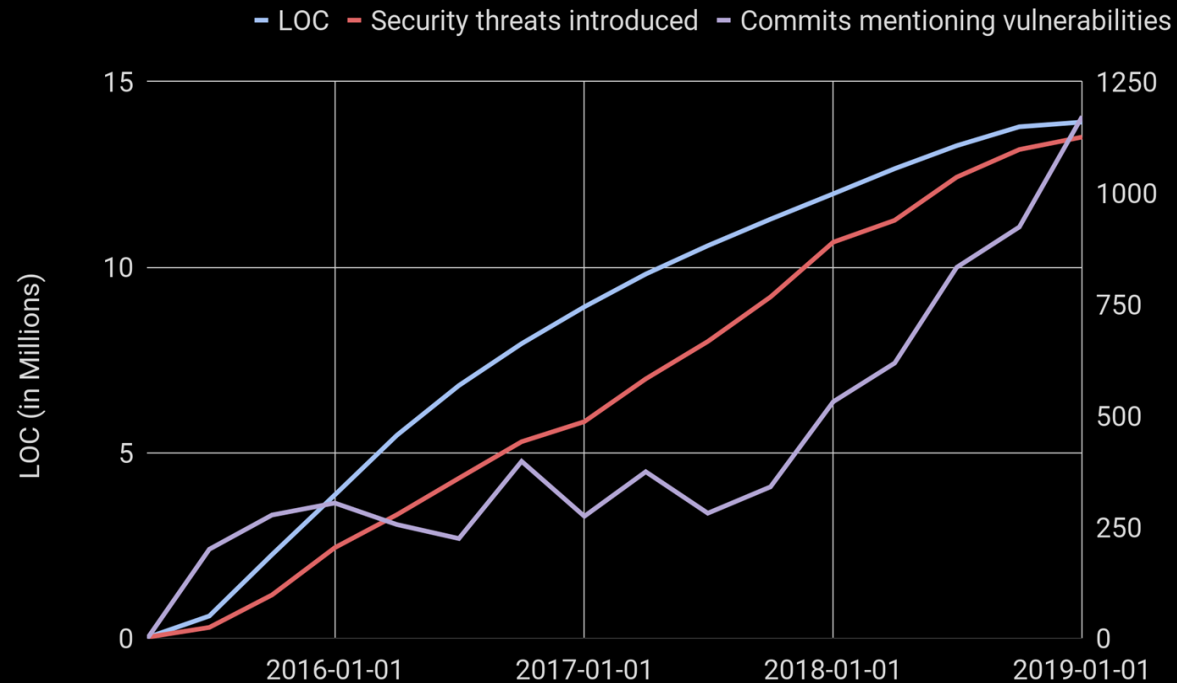


Why DevOps Security?



More code = more technical debt & exposure

Security threats continue to rise with LOC



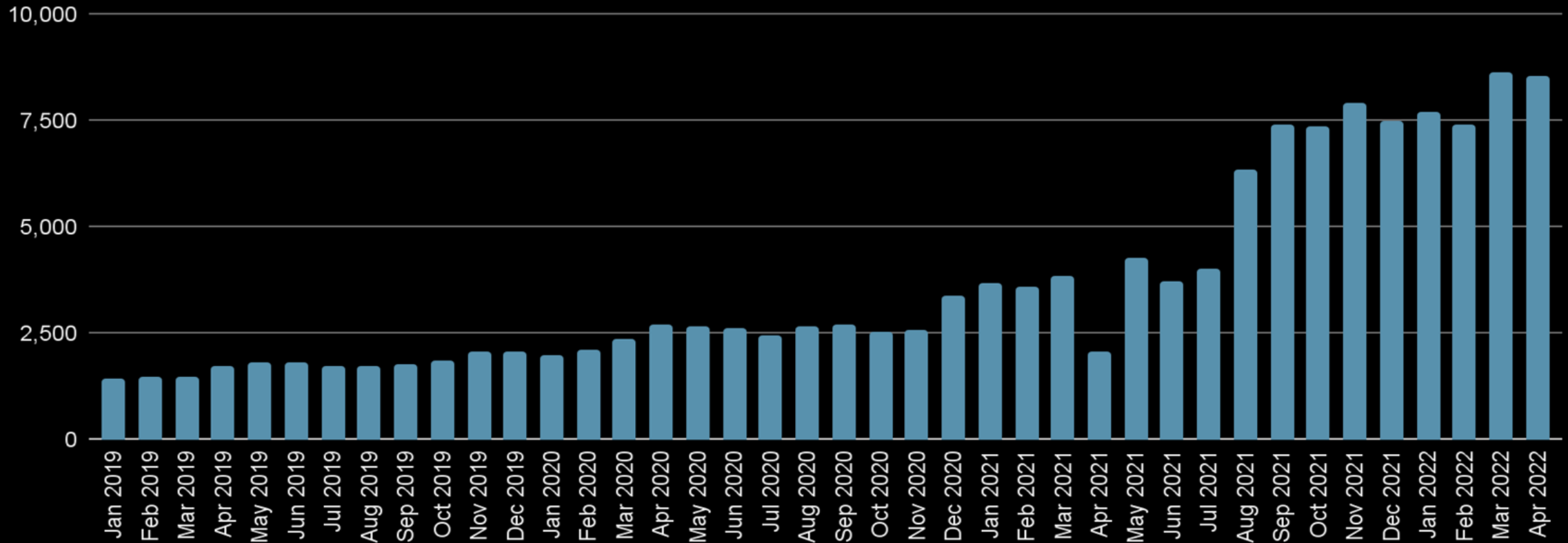
Flaws in applications are consistently the #1 attack vector for breaches

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

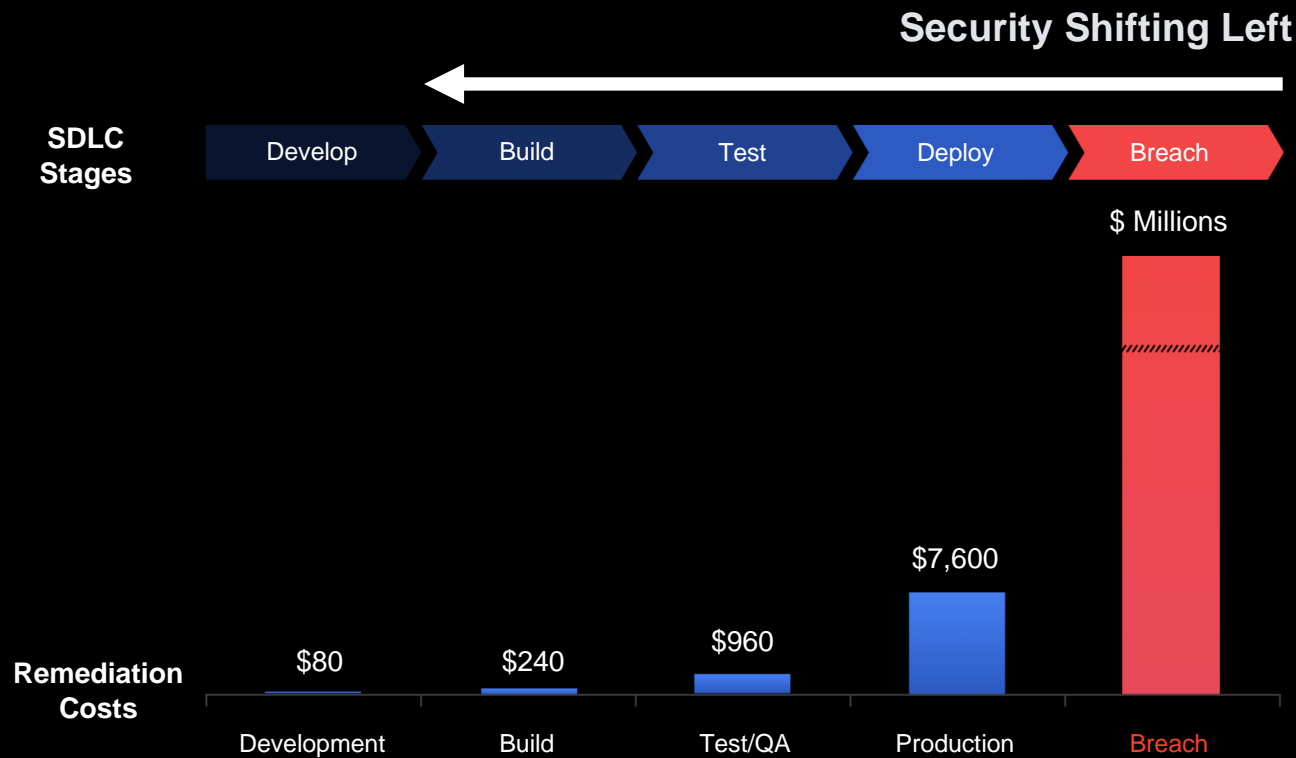
Source: Verizon Data Breach Investigations reports 2016, 2017, 2018, 2019 and 2020.

We're seeing more credential leaks than ever

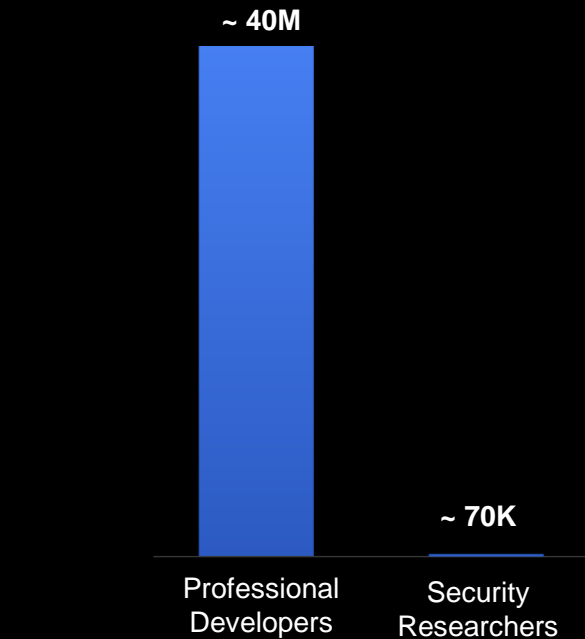
GitHub access tokens leaked in public repositories



Shifting security left, but why?

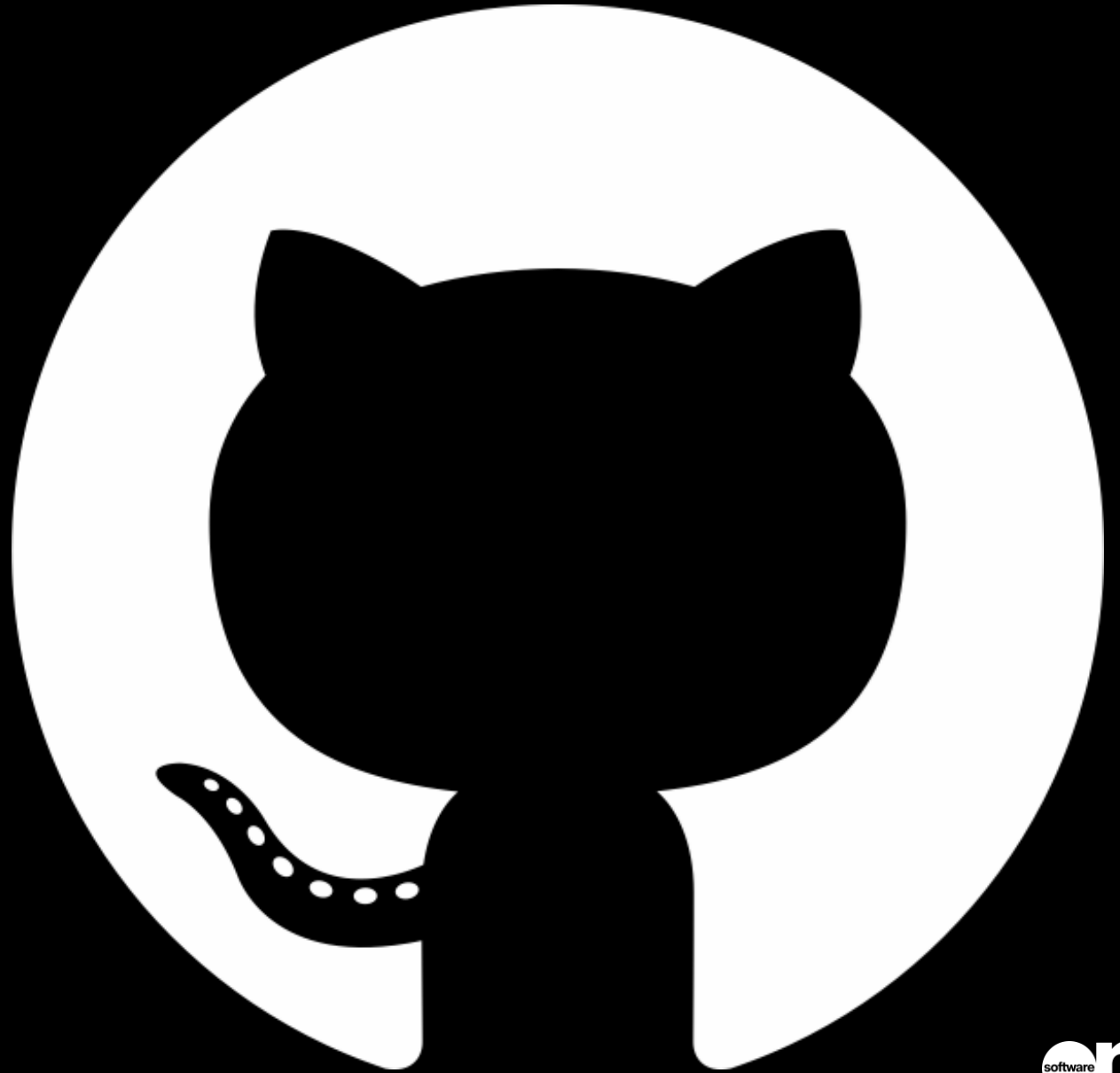


Vastly more cost effective to remediate during development



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

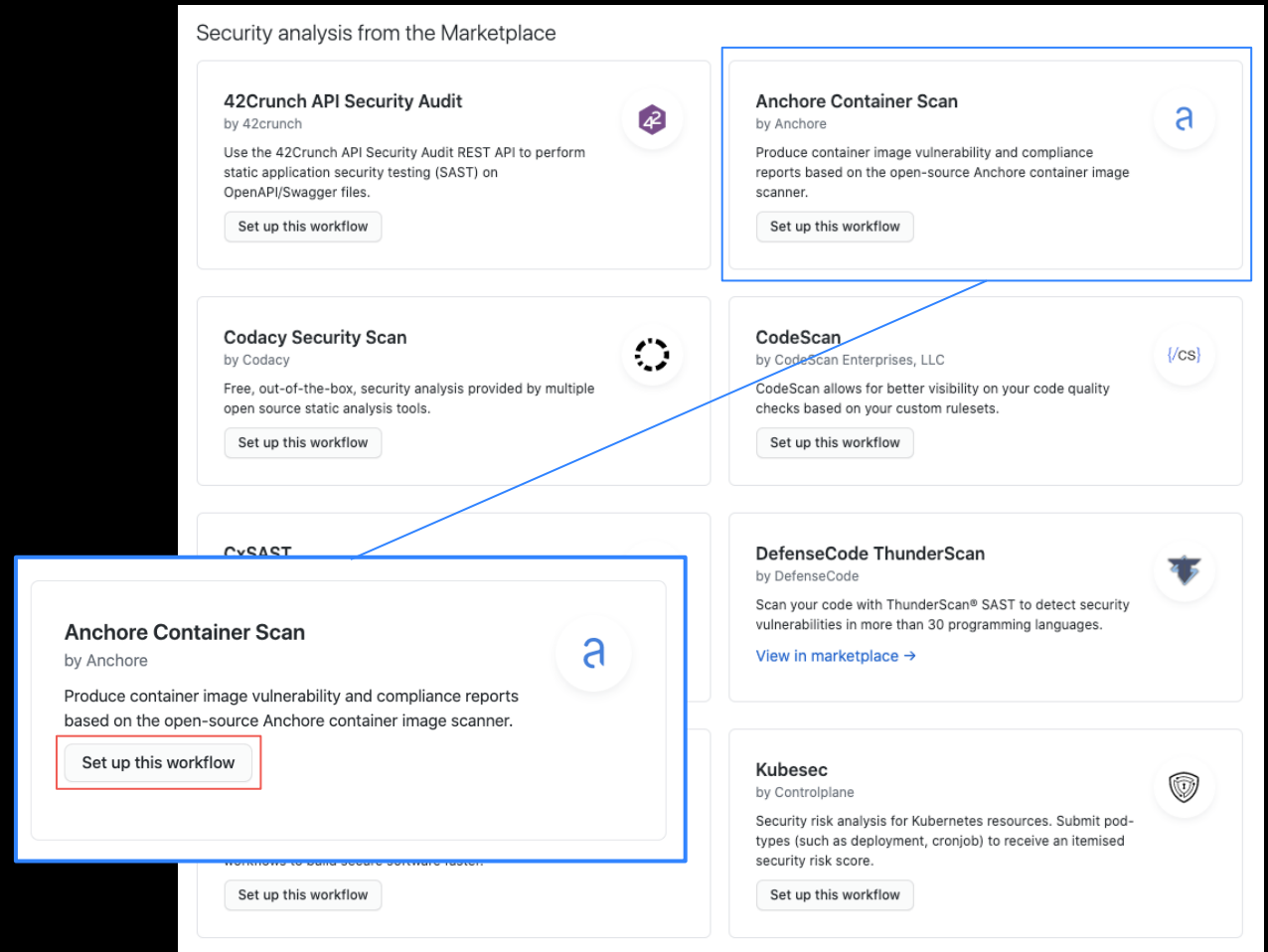
Share security knowledge within your teams using codified, readable and executable queries



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**

Dependabot alerts				Dismiss all ▾
30 Open ✓ 0 Closed		Manifest ▾	Sort ▾	
⚠️ jquery	18 Jan 2021 by GitHub	app/public/js/jquery.min.js	moderate severity	
⚠️ bl	18 Jan 2021 by GitHub	app/package-lock.json	high severity	
⚠️ decompress	18 Jan 2021 by GitHub	app/package-lock.json	high severity	
⚠️ mongodb	18 Jan 2021 by GitHub	app/package-lock.json	high severity	
⚠️ base64url	18 Jan 2021 by GitHub	app/package-lock.json	moderate severity	
⚠️ is-my-json-valid	18 Jan 2021 by GitHub	app/package-lock.json	low severity	
⚠️ minimist			low severity	

⚠️ This automated pull request fixes a [security vulnerability](#)

Only users with access to Dependabot alerts can see this message. [Learn more about Dependabot security updates](#), [opt out](#), or [give us feedback](#).

moderate severity

Secure your supply chain

Fix and publish vulnerability information

- SECURITY.md
- Security Advisories
- GitHub Advisory Database

The screenshot shows the GitHub interface for the tensorflow/tensorflow repository. The 'Security' tab is selected, displaying a list of 35 published security advisories. The left sidebar shows navigation options: Overview, Security policy, and Security advisories (35). The main content area lists several advisories with their titles, IDs, publication dates, authors, and severity levels.

Advisory Title	ID	Published On	Author	Severity
✓ Heap out of bounds access in MakeEdge	GHSA-q263-fvxn-m5mw	9 Dec 2020	mihairuseac	high severity
✓ CHECK-fail in LSTM with zero-length input	GHSA-m648-33qf-v3gp	9 Dec 2020	mihairuseac	low severity
✓ Heap out of bounds read in filesystem glob matching	GHSA-9jjw-hf72-3mxw	9 Dec 2020	mihairuseac	critical severity
✓ Write to immutable memory region	GHSA-hhvc-g5hv-48c6	9 Dec 2020	mihairuseac	low severity
✓ Lack of validation in data format attributes	GHSA-c9f3-9wfr-wgh7	9 Dec 2020	mihairuseac	low severity
✓ Uninitialized memory access in Eigen types	GHSA-qhxx-j73r-qpm2	9 Dec 2020	mihairuseac	low severity

Secure your supply chain

Dependency Review

- Review Dependency
- Feedback in Pull Request
- Dependency Licensing

484

docs/package-lock.json

<>

Viewed

...

+

json-logic-js

1.2.3

released 7 months ago

875

Prototype Pollution in json-logic-js (GHSA-m9hw-7xfv-wqg7)

high severity

Patched version: 2.0.0

+

emoji-regex

7.0.3

released 2 years ago

5.78m

MIT

+

locate-path

3.0.0

released 3 years ago

7.6m

MIT

+

p-limit

2.3.0

released 14 months ago

7.64m

MIT

7.6m

MIT

7.2m

MIT

8.33m

6.92m

GHSA-m9hw-7xfv-wqg7)

+ json-logic-js 1.2.3 released 7 months ago

Prototype Pollution in json-logic-js (GHSA-m9hw-7xfv-wqg7)

high severity Patched version: 2.0.0

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

The screenshot displays the GitHub Security Center interface. At the top, there are tabs for 'Security' (with 69 items), 'Insights', and 'Settings'. Below these, the title 'GitHub Personal Access Token' is shown with an 'Open' button and the text 'GitHub detected on 13 Aug 2020'. A 'Mark as' dropdown menu is open, showing options: 'Revoked', 'False positive', 'Used in tests', and 'Won't fix'. Below the title, there are tabs for 'Details' and 'Files' (with 1 file). The code file 'src/index.js' is open, showing the following code:

```
2
3 let auth_key = 'fb50ec73d7366c487248b80e1f97a8b2ec550b82'
4 var token = "8256ba5a40014ed318f8f22cc15227b579e341ef"
5 var token2 = '9278b9f396e023a0680f6100ce9371b2e7619827'
```

The line containing the token is highlighted in yellow. Below the code, a message states: 'If this secret is valid, we recommend that you rotate it and then revoke it. Committed secrets can be discovered by anyone with read access to your code, potentially resulting in unauthorized access to the services you use. Once you've revoked this secret, close it as revoked here. You can also report it as a false positive or a testing secret, or just ignore it.' The text 'GitHub Personal Access Token' is also visible at the bottom of the message box.



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

Security & analysis / New custom pattern

Custom pattern name

Your custom pattern

Secret format

The pattern for the secret, specified as a regular expression. [Learn more.](#)

example_`[A-Za-z0-9]{40}`

More options ▾

Test string

Secret scanning

Receive alerts when secrets or keys are checked in.

Disable

1 Custom pattern

RSA Key

Created 24 minutes ago by niroschan

Remove

⊕ Add a secret scanning custom pattern

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!

Active 17 CS Chad Bentz(felickz) 102-fix-code-scanning-alert-polynomial-regular-expression-used-on-uncontrolled-data into master CS NL

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!

Show everything (4)

Add a comment...

Chad Bentz(felickz) made Nicholas Liffen a required reviewer 7m ago

Approve

Set auto-complete

Reviewers

Required

Nicholas Liffen

No review yet

Optional

Chad Bentz(felickz)

No review yet

Tags

New Feature

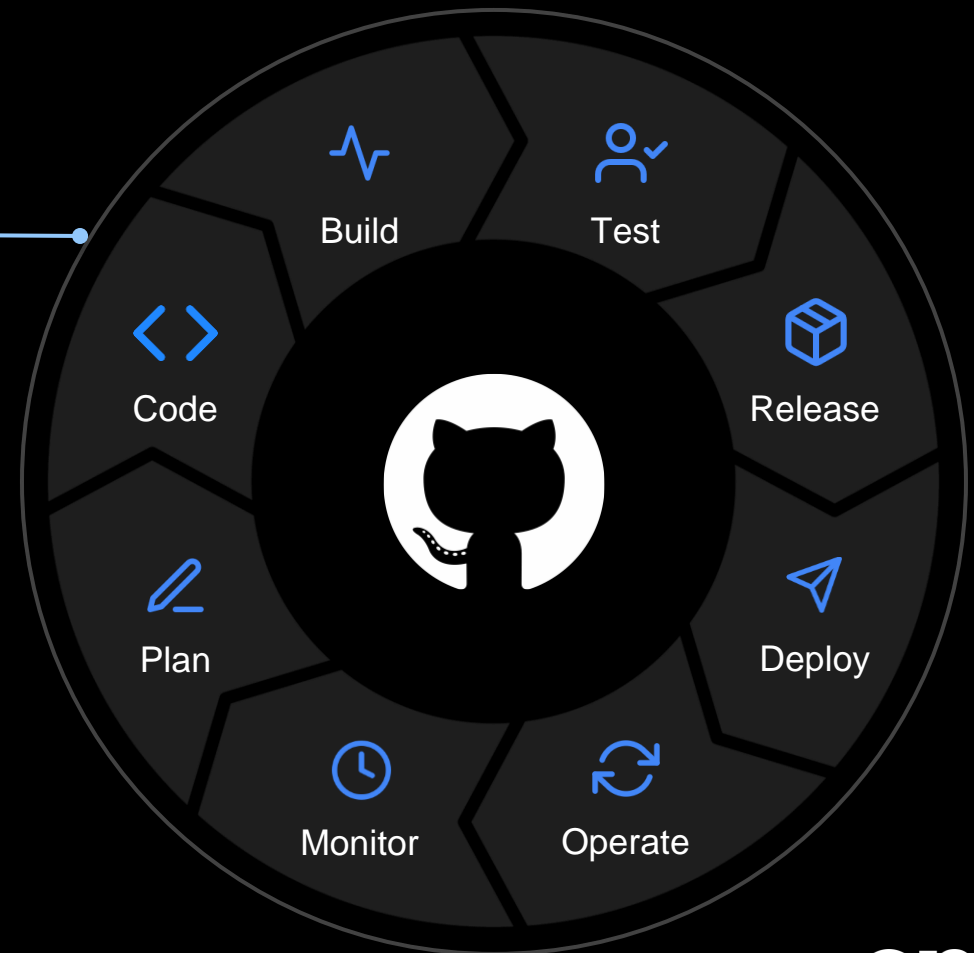
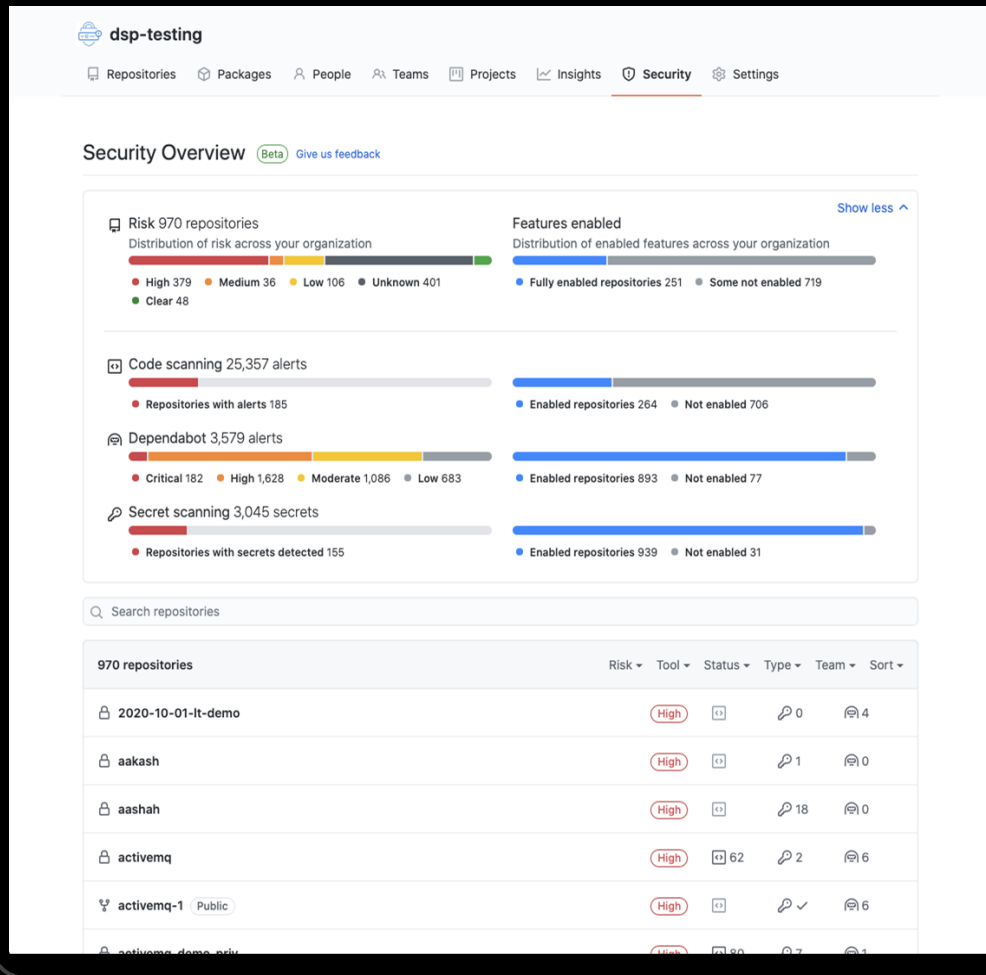
Work items

Task 30: Create New Feature

Updated Yesterday, Doing

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

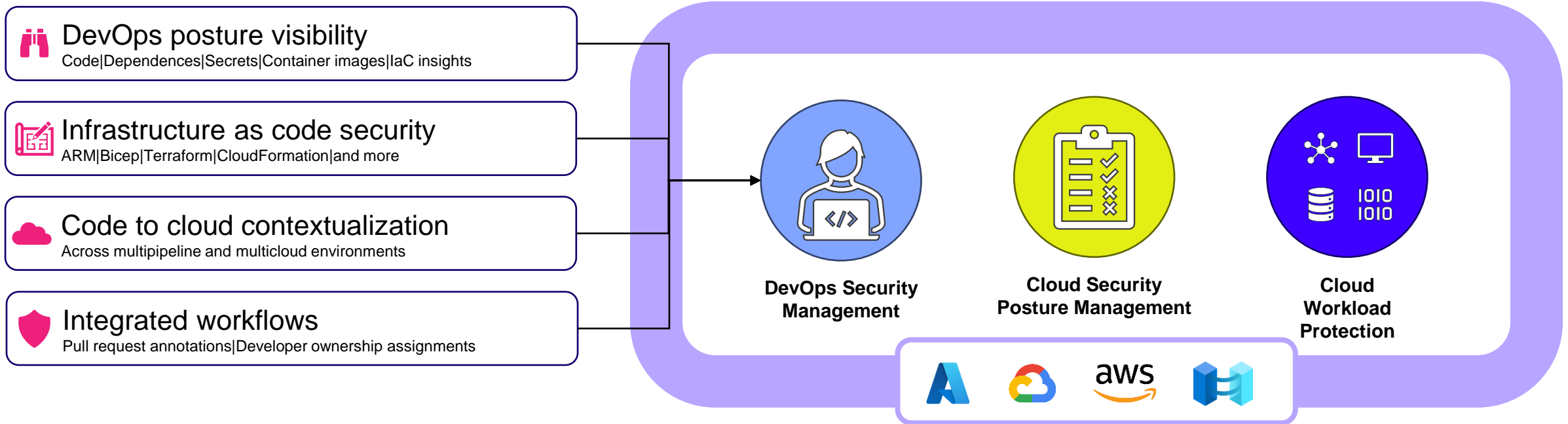
**Do you really
believe Ops
people use
GitHub?**



What about Defender for Cloud?



It supports DevOps environments!



GitHub Copilot

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



GitHub Copilot Enterprise – PR Review

The screenshot shows a GitHub Pull Request (PR) interface. At the top, the repository is 'octodemo / geektrainer-demo-conference'. The PR title is 'Add Django messages to submit and edit flows #12'. The PR is open, showing 1 commit from the 'add-success-messages' branch to the 'main' branch. The PR description is 'Resolves issue'. The PR is reviewed by 'GeekTrainer' 7 hours ago. The PR is still in progress, with a 'Convert to draft' button. The PR has 11 additions and 2 deletions. The PR is assigned to 'No one' and has no labels. The PR is still in progress, with a 'Convert to draft' button. The PR has 11 additions and 2 deletions. The PR is assigned to 'No one' and has no labels.

octodemo / geektrainer-demo-conference

Type to search

Code Issues 1 Pull requests 1 Discussions Actions Projects Wiki Security Insights

Add Django messages to submit and edit flows #12

Edit <> Code

Open GeekTrainer wants to merge 1 commit into main from add-success-messages

Conversation 0 Commits 1 Checks 0 Files changed 2 +11 -2

GeekTrainer commented 7 hours ago • edited

Resolves issue

🔗 Add Django messages to submit and edit flows 0fb4de0

Add more commits by pushing to the add-success-messages branch on octodemo/geektrainer-demo-conference.

Reviewers

No reviews

Still in progress? [Convert to draft](#)

Assignees

No one—[assign yourself](#)

Labels

None yet

Thank you and...

Vota Lorenzo!

lorenzo.barbieri@
softwareone.com

