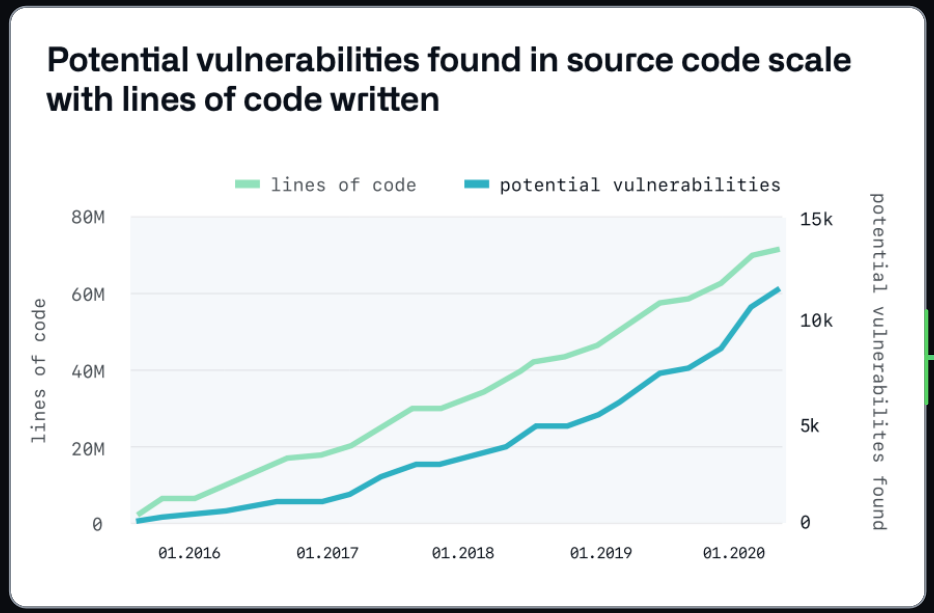
GitHub Advanced Security for Developers

The state of AppSec



Despite billions of dollars of investment…

85% of applications still contain a security issue

Code written in 2020 is just as likely to introduce a security issue as code written in 2016

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

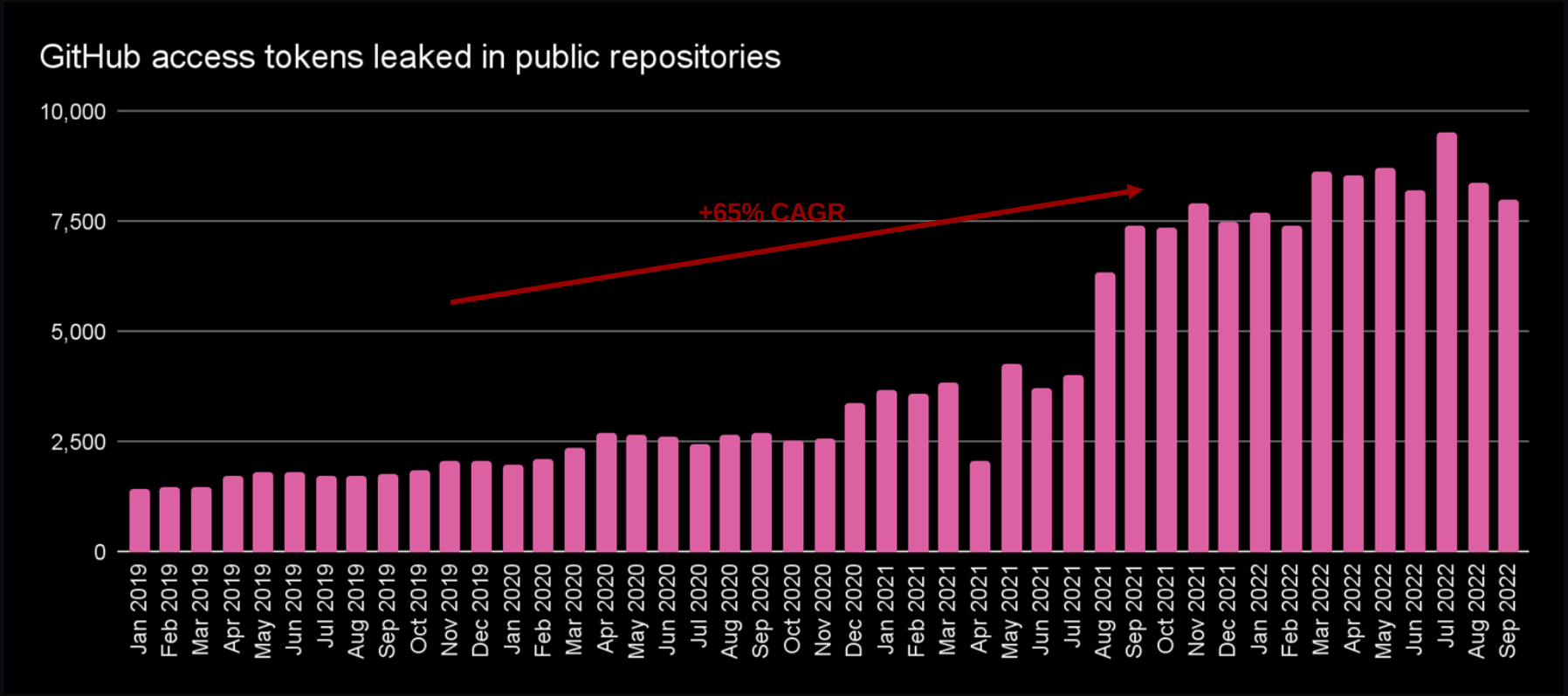
Source: Verizon Data Breach Investigations reports 2016, 2017, 2018, 2019 and 2020.

The state of AppSec

Is falling further behind the current state of Development

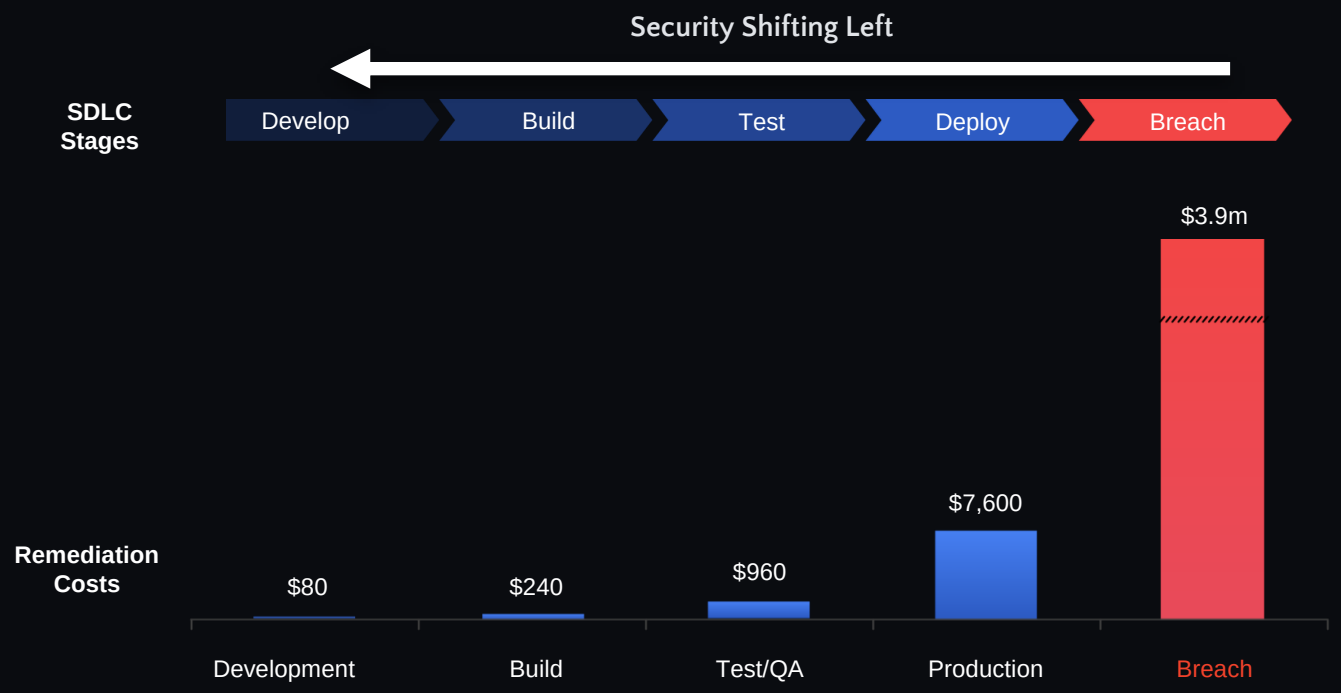
- 1:100 Security team members to developers
- Lack of knowledge voted the main AppSec challenge
- Remediation trends are stagnant

We’re seeing more credential leaks than ever



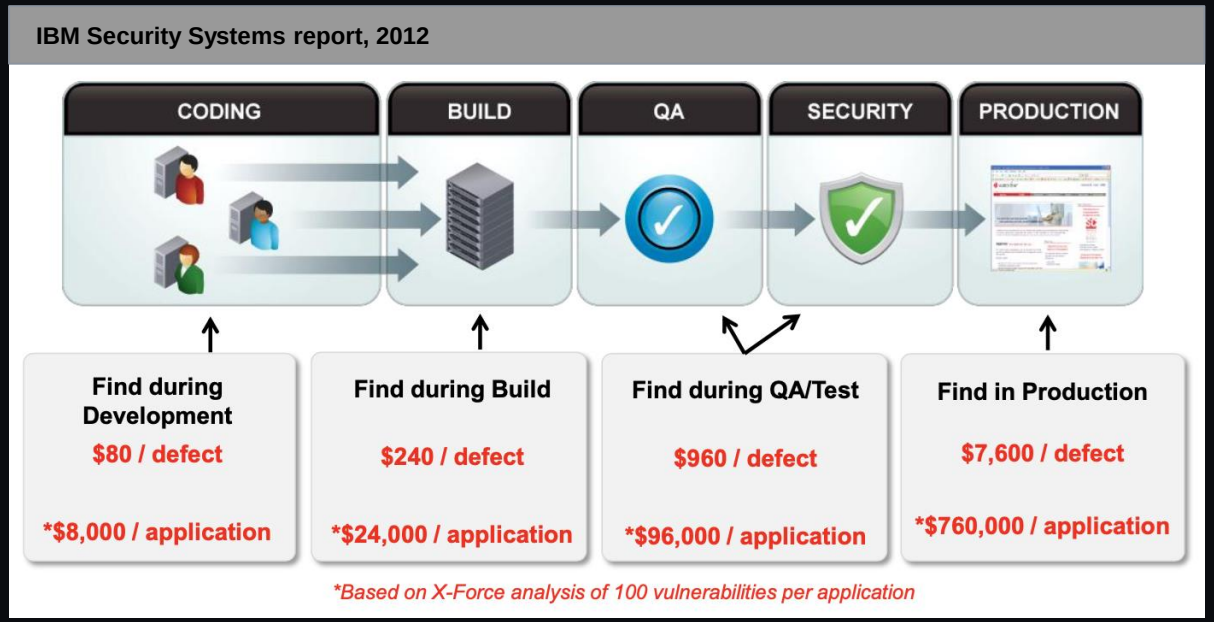
Source: GitHub data

Everyone wants to shift security left…



Source: Ponemon Institute Cost of a Data Breach 2020

… but the industry has been trying to shift left for at least a decade



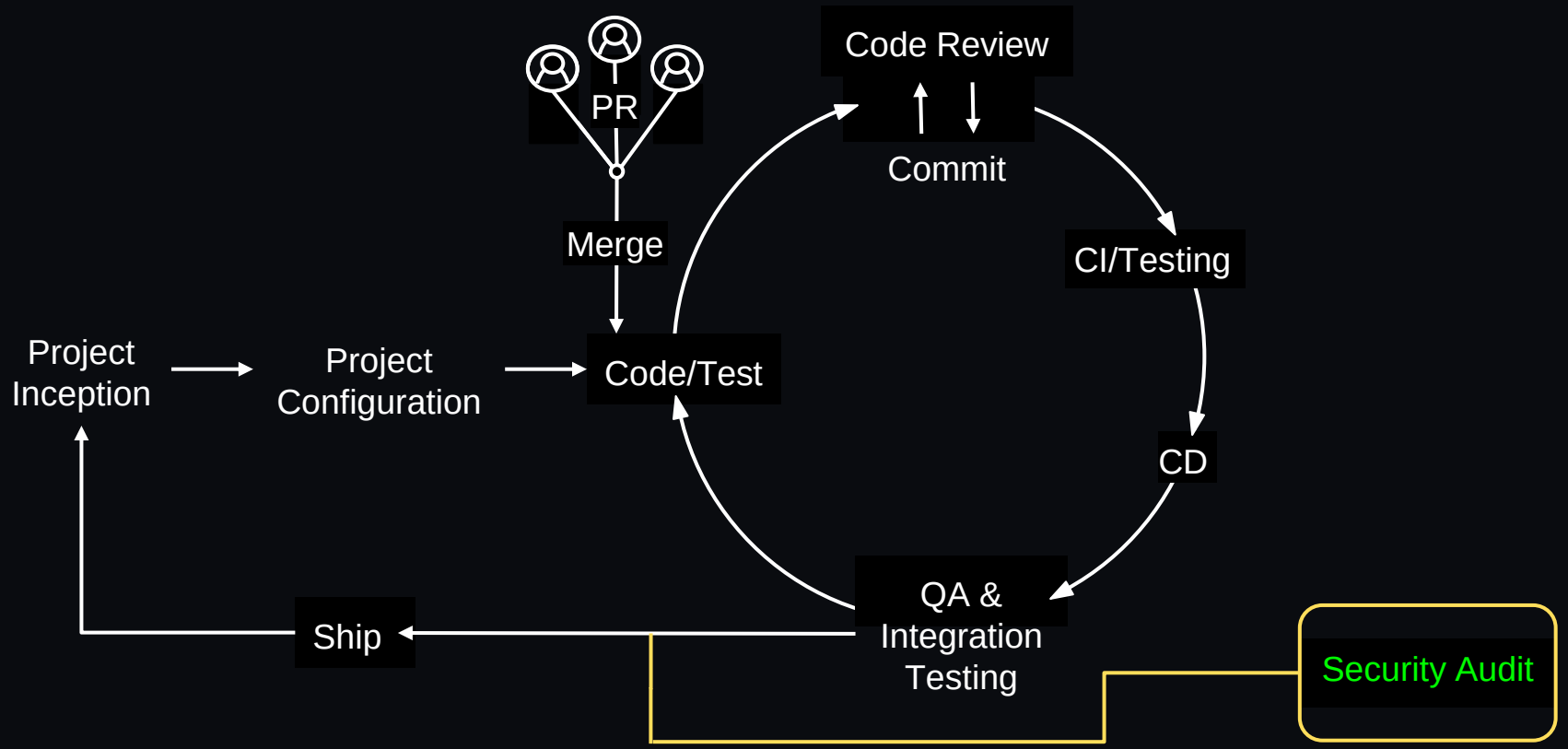
GitHub believes that making this shift requires a developer-first approach to all our security products:

- Integrate *directly* into the developer workflow.

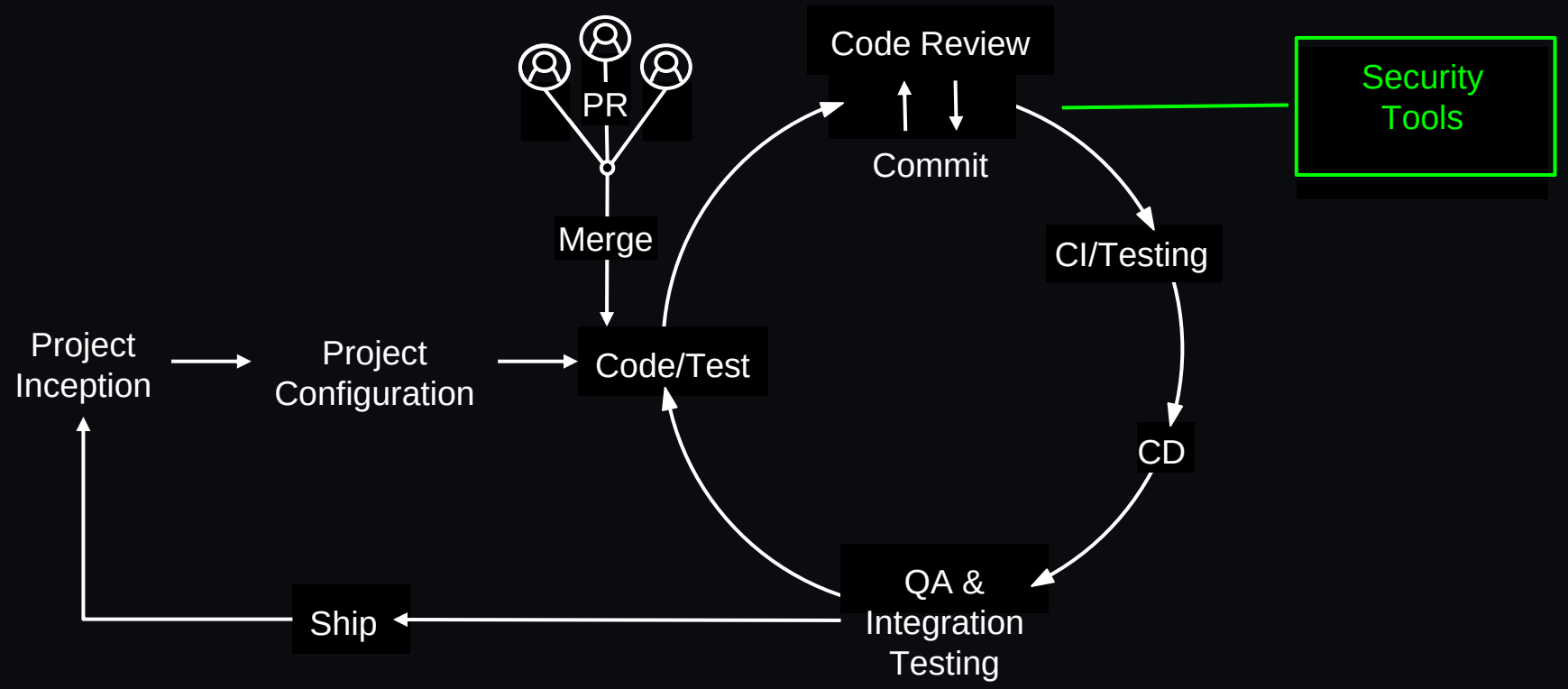
- Make setup and deployment fast and easy.

- Produce high quality results with low numbers of false positives.

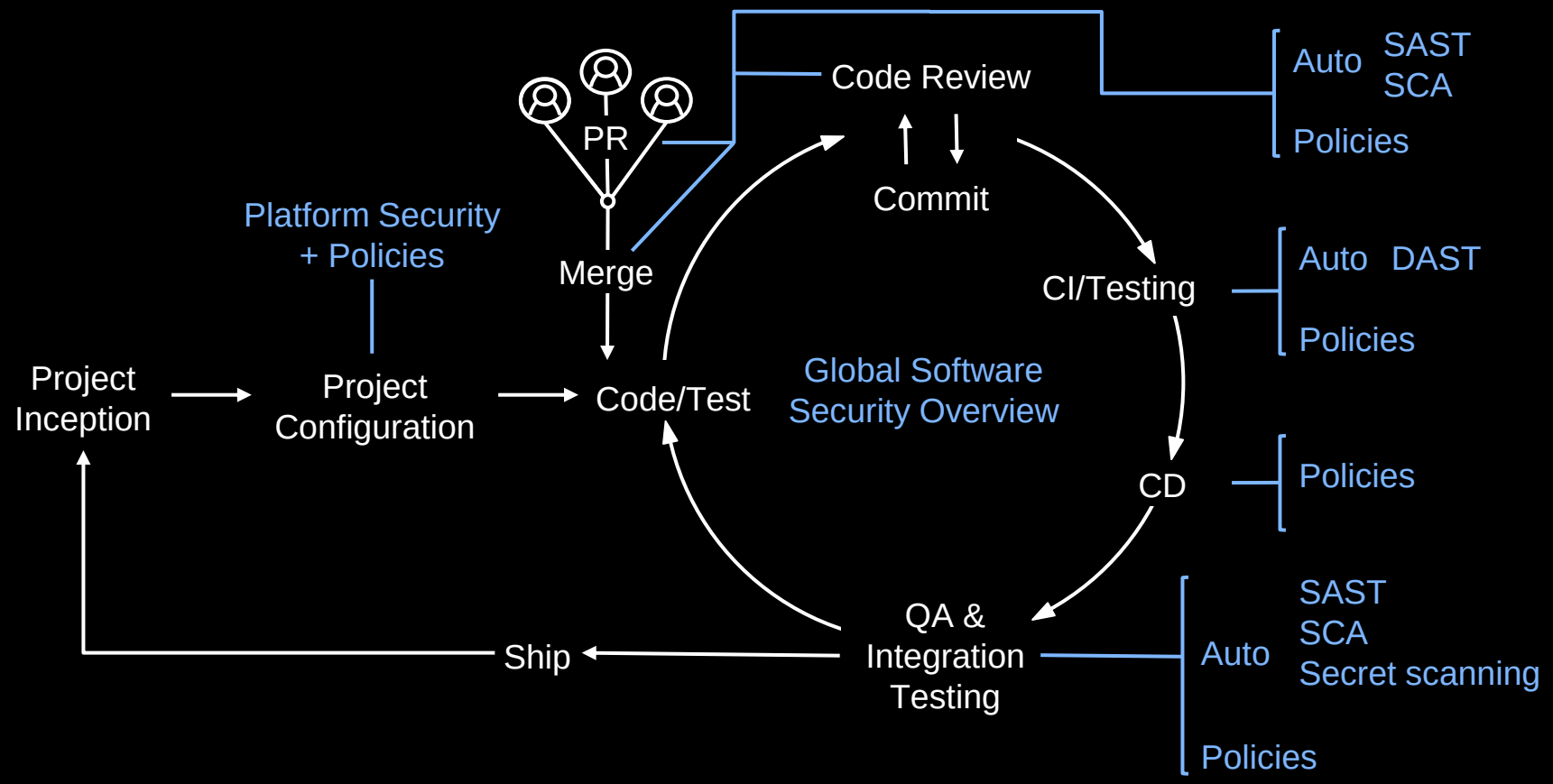
Basic Application Security scenario



Application Security scenario



Application Security - Targeted state



Developer first?

We see three key aspects to being a “developer first” tool:

Integrate *directly* into the developer workflow.

Make setup and deployment fast and easy.

Produce high quality results with low numbers of false positives.

GitHub Advanced Security: Current capabilities

supply chain

Dependency graph
View your dependencies

Advisory database
Canonical database of dependency vulnerabilities

Security alerts and updates
Notifications for vulnerabilities in your dependencies, and pull requests to fix them

Dependency review
Identify new dependencies and vulnerabilities in a PR

code

Secret scanning
Find API tokens or other secrets exposed anywhere in your git history.

Code scanning
Static analysis of every git push, integrated into the developer workflow and powered by CodeQL

platform

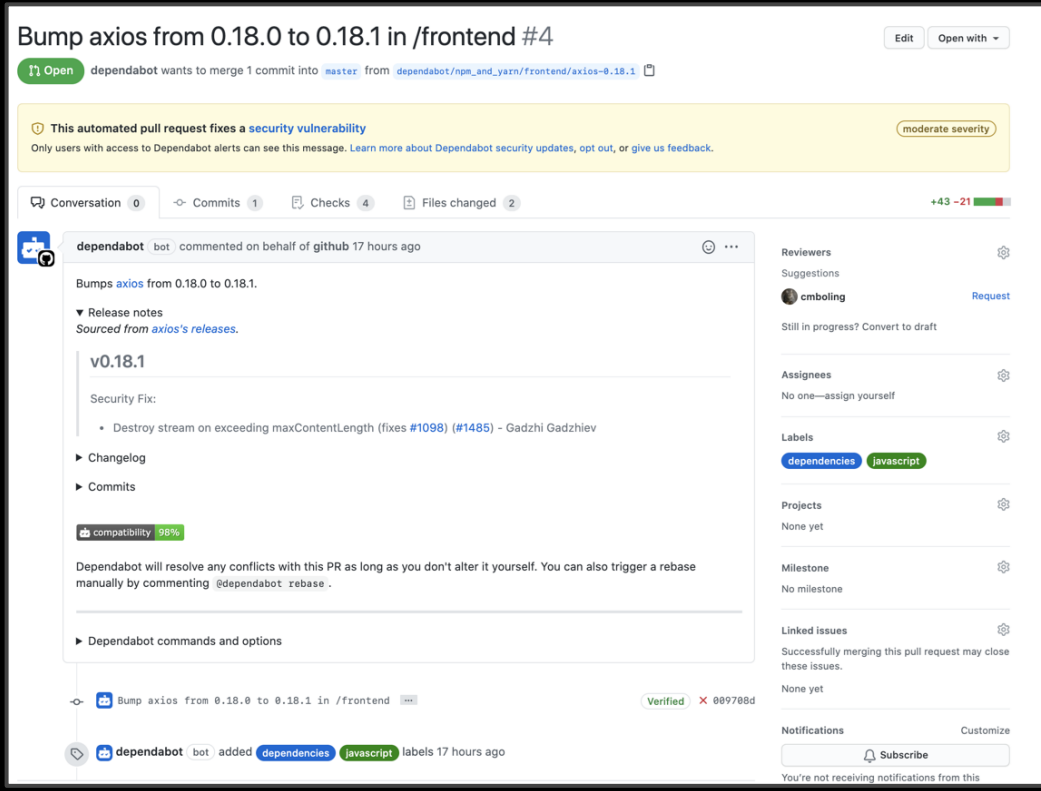
Branch protection
Enforce requirement for pushing to a branch or merging PRs

Commit signing
Enforce requirement that all commits are signed

Security overview
View security results of all kinds across your organization

Dependabot

- Developers (and others!) notified by an alert when new vulnerable dependencies are detected.
- Automatically open pull requests to fix dependency vulnerabilities.
- Supports dependency review within PRs to prevent adding known vulnerable dependencies.

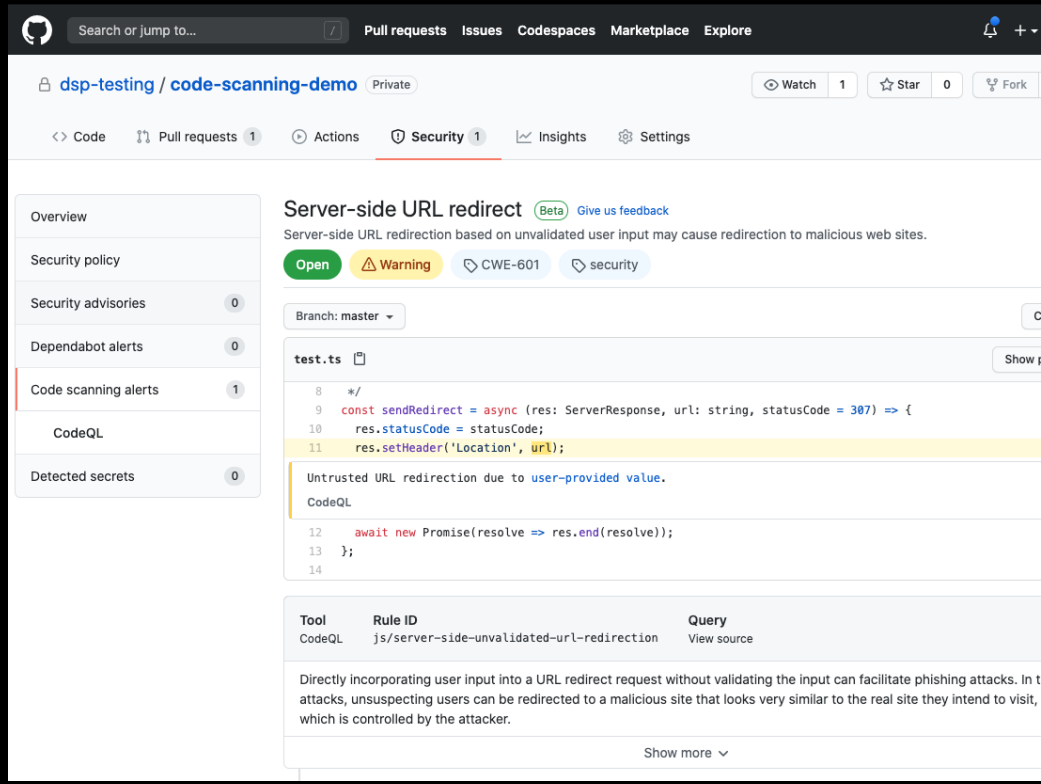


Secret scanning

- Identify secrets across your entire git history with high accuracy.
- Push protection - prevent secrets from being pushed to GitHub.
- Developers (and others!) notified by an alert if secrets are pushed.
- Automated revocation for public repositories, private repositories include a review workflow.

Code scanning

- Find vulnerabilities before they are merged into the code base with automated CodeQL scans
- Integrate results directly into the developer workflow
- Run custom queries and the community-powered GitHub query set
- Extensible, with support for other SAST tools



Reviewing Alerts

Overview | Repositories | Projects | Packages | Teams | People | Security | ...

Security

- Overview (Beta)
- Risk
- Coverage

Metrics

- Secret scanning (Beta)

Alerts

- Dependabot 0
- Code scanning 0
- Secret scanning 0

You can only see data from repositories for which you have permission to view.

Overview

Give feedback

Alert trends and insights across your organization.

Dec 15, 2023 - Jan 14, 2024

Filter

Try modifying your filters to see the security impact on your organization.

Monitoring and responding to alerts

Code samples for "List code scanning alerts for an organization"

Request example

GET /orgs/{org}/code-scanning/alerts

cURL | JavaScript | GitHub CLI

```javascript
// Octokit.js
// https://github.com/octokit/core.js#readme
const octokit = new Octokit({
  auth: 'YOUR-TOKEN'
})

await octokit.request('GET /orgs/{org}/code-scanning/alerts', {
  org: 'ORG',
  headers: {
    'X-GitHub-Api-Version': '2022-11-28'
  }
})
```

Q&A