Securing the Software Factory

Jon Peck
Sr Manager, Enterprise Advocacy at GitHub

GitHub is the largest developer platform on Earth

94M+	200M+	1,000s	2.6B+	4M+	90%
Developers	Private and public repositories	Top open source communities	Contributions per year	Organizations	Fortune 100 companies

A **fully integrated platform** from idea-to-production

Collaborative, automated workflows

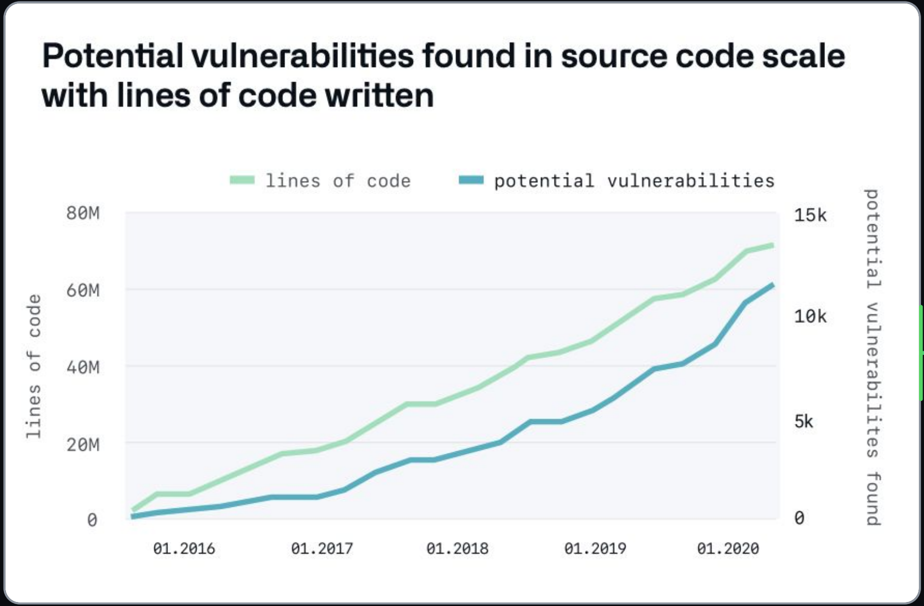
Seamless access to OSS and Innersource

Developer focused security and compliance

Deploy anywhere including your own data centers

The State of AppSec

More code = more problems


Potential vulnerabilities found in source code scale with lines of code written

Despite billions of dollars of investment…

85% of applications still contain a security issue

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

The State of AppSec

+80% of code bases are open source

Essential to secure your use of open source end to end

Too few secure developers

44% of developers are not trained to code securely

Companies struggle to adopt DevSecOps

93% of DevSecOps implementations are **not** optimized

Sources: BLS, NSF, NCES, IDC, Gartner, LinkedIn, C+AI Corp Strat

Source: DORA State of Devops Report 2018

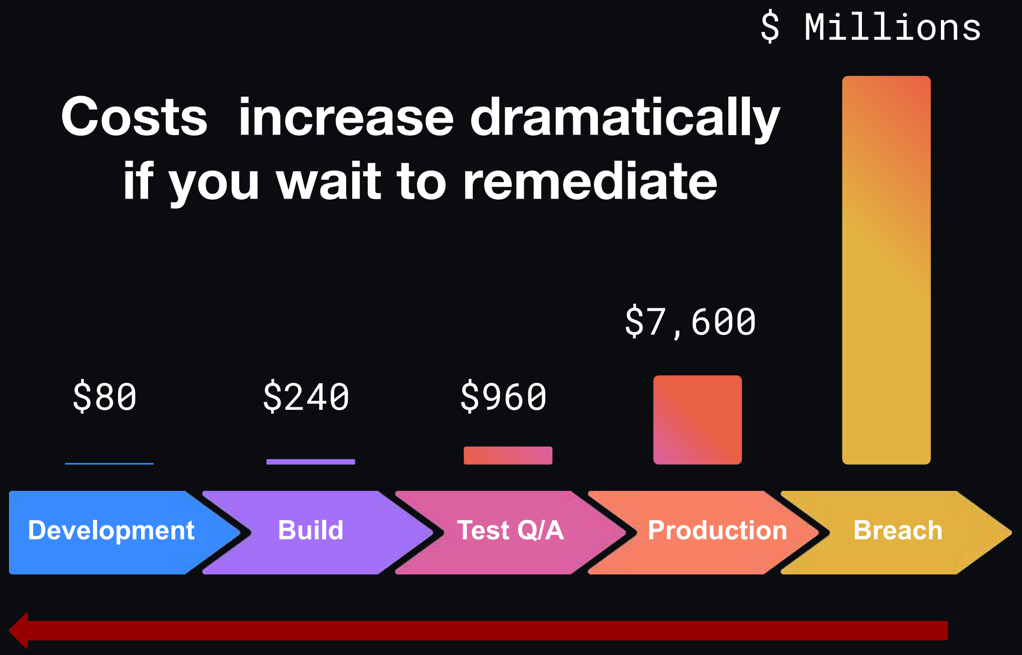
The State of AppSec

50% of Companies

sacrifice cybersecurity for speed

57% of ops teams

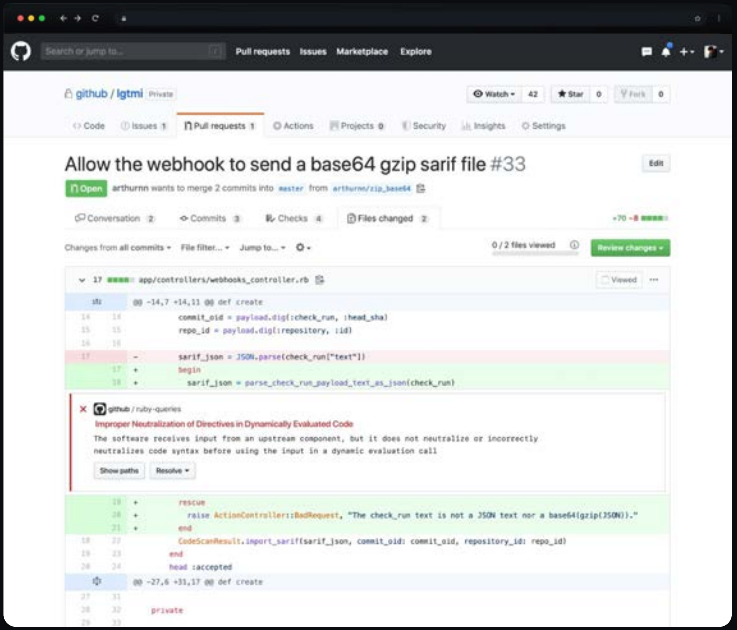
push back on security practices



Costs increase dramatically if you wait to remediate

Sources: Threat Stack 2018,
NIST, Polemon Institute

Build security right into the Developer Lifecycle



Allow the webhook to send a base64 gzip sarif file #33

arthurnn wants to merge 2 commits into `master` from `arthurnn/zip_base64`

17 app/controllers/webhooks_controller.rb

```
@@ -14,7 +14,11 @@ def create
          commit_oid = payload.dig(:check_run, :head_sha)
          repo_id = payload.dig(:repository, :id)

-         sarif_json = JSON.parse(check_run["text"])
+         begin
+           sarif_json = parse_check_run_payload_text_as_json(check_run)
```

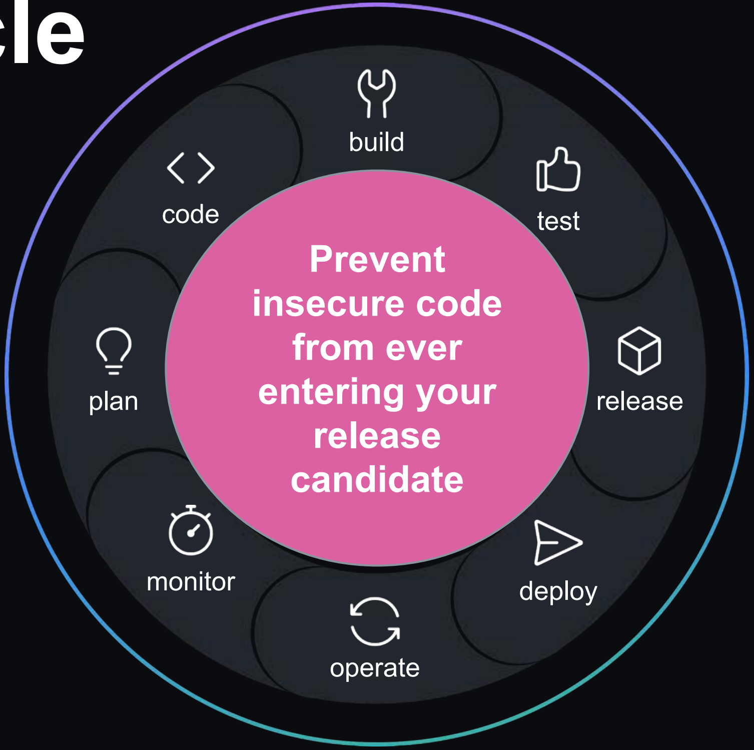
github / ruby-queries

Improper Neutralization of Directives in Dynamically Evaluated Code

The software receives input from an upstream component, but it does not neutralize or incorrectly neutralizes code syntax before using the input in a dynamic evaluation call

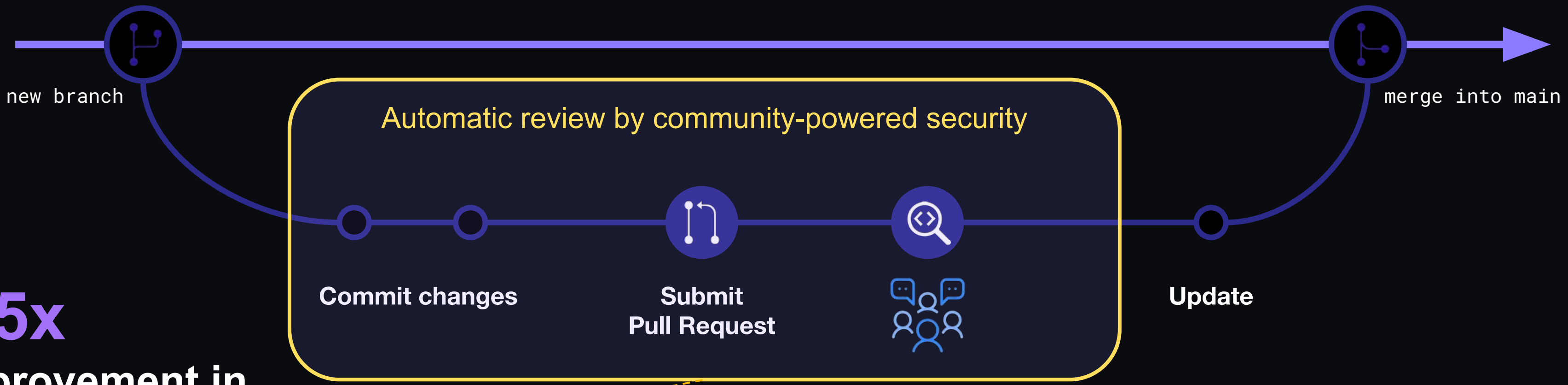
```
+         rescue
+           raise ActionController::BadRequest, "The check_run text is not a JSON text nor a base64(gzip(JSON))."
+         end
          CodeScanResult.import_sarif(sarif_json, commit_oid: commit_oid, repository_id: repo_id)
        end
        head :accepted
@@ -27,6 +31,17 @@ def create

      private
```



Prevent insecure code from ever entering your release candidate

Proactive AppSec



4.5x

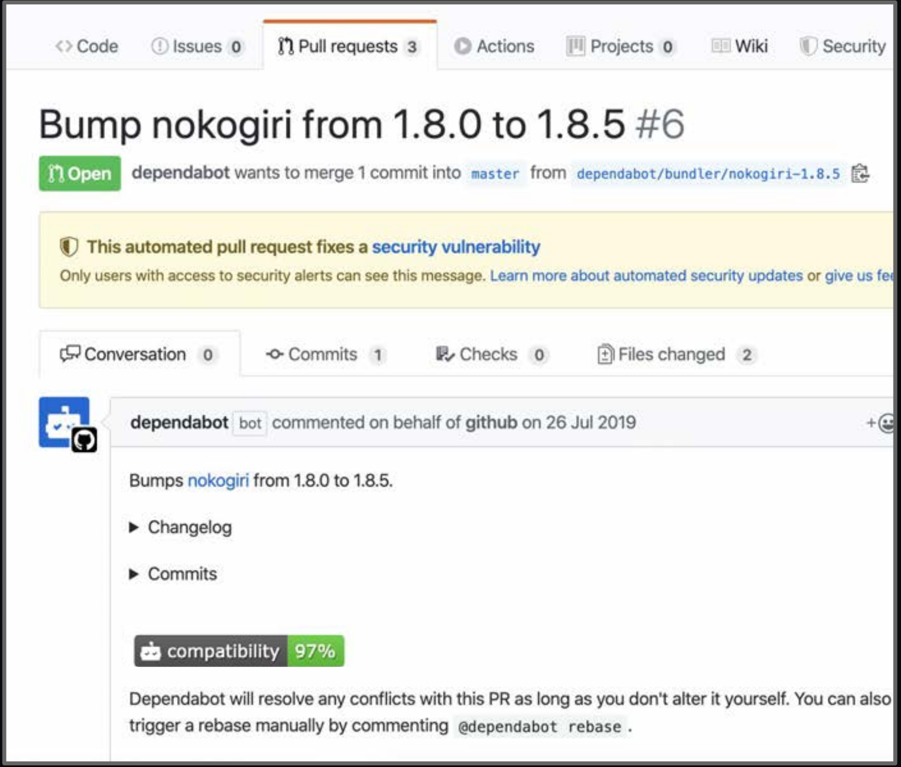
improvement in

remediation time

Dependency Scanning: automatic
CVE identification & remediation

Dependency Scanning & Automatic Security Updates

- Find vulnerabilities before they are merged into the code base
- Automatically generate suggested fix for 1-click resolution
- Severity level, vulnerability detail, and fix compatibility score
- Realtime CVE inventory from National Vulnerability Database (NIST) + GitHub Advisory Database



Bump nokogiri from 1.8.0 to 1.8.5 #6

Open dependabot wants to merge 1 commit into `master` from `dependabot/bundler/nokogiri-1.8.5`

This automated pull request fixes a security vulnerability

Only users with access to security alerts can see this message. Learn more about automated security updates or give us fe

dependabot bot commented on behalf of github on 26 Jul 2019

Bumps nokogiri from 1.8.0 to 1.8.5.

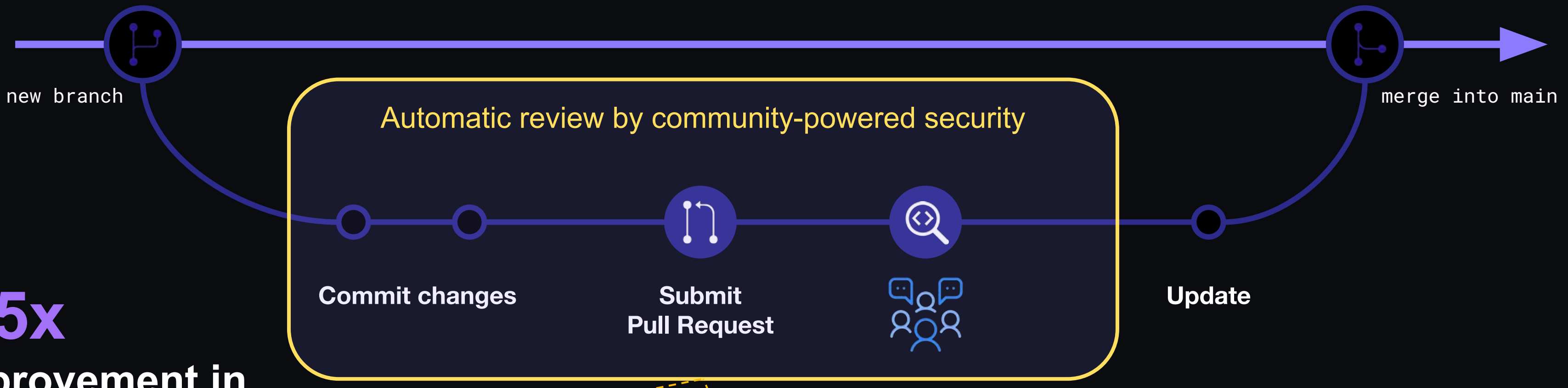
▶ Changelog

▶ Commits

compatibility 97%

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

Proactive AppSec



4.5x
improvement in
remediation time

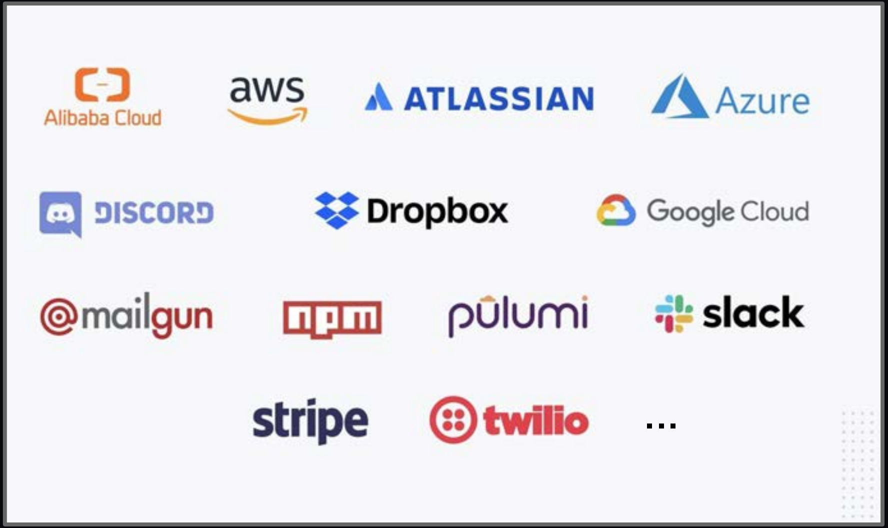
Dependency Scanning: automatic CVE identification & remediation

Secret Scanning: locate and invalidate exposed tokens

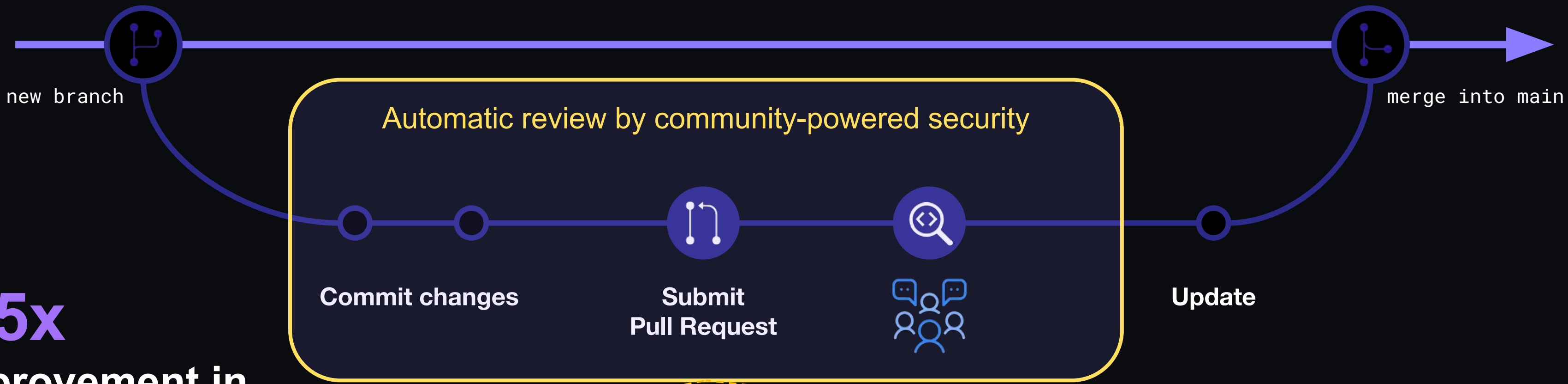
Blocked at push
+ historic remediation

Secret Scanning for private repositories

- Find secrets ***before*** they’re pushed to GitHub
- Scan your entire git history
- Easily exclude false positives
- Custom secret patterns
- Bulk triage



Proactive AppSec



new branch

merge into main

Automatic review by community-powered security

Commit changes

Submit
Pull Request

Update

4.5x
improvement in
remediation time

Dependency Scanning: automatic CVE identification & remediation

Secret Scanning: locate and invalidate exposed tokens

Blocked at push
+ historic remediation

Stakes were extremely high...

$2.5B

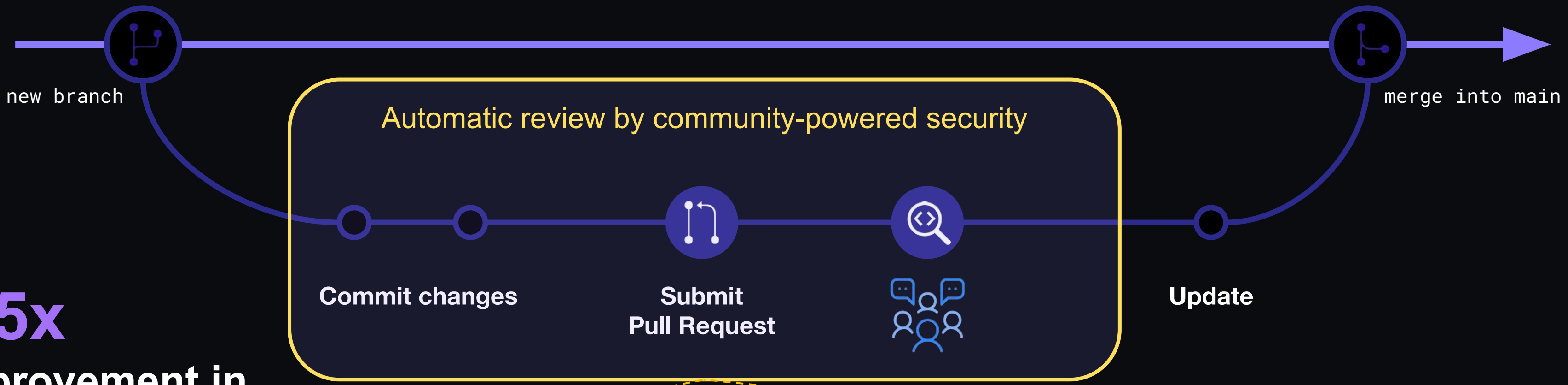
Total estimated project cost

> "It could take the entire Mars program down with it. It is victory or death."
>
> Robert Zubrin

CodeQL to the rescue!

30 bug variants found & fixed

Proactive AppSec



new branch

merge into main

Automatic review by community-powered security

Commit changes

Submit
Pull Request

Update

4.5x
improvement in
remediation time

Dependency Scanning: automatic CVE identification & remediation

Secret Scanning: locate and invalidate exposed tokens

Blocked at push
+ historic remediation

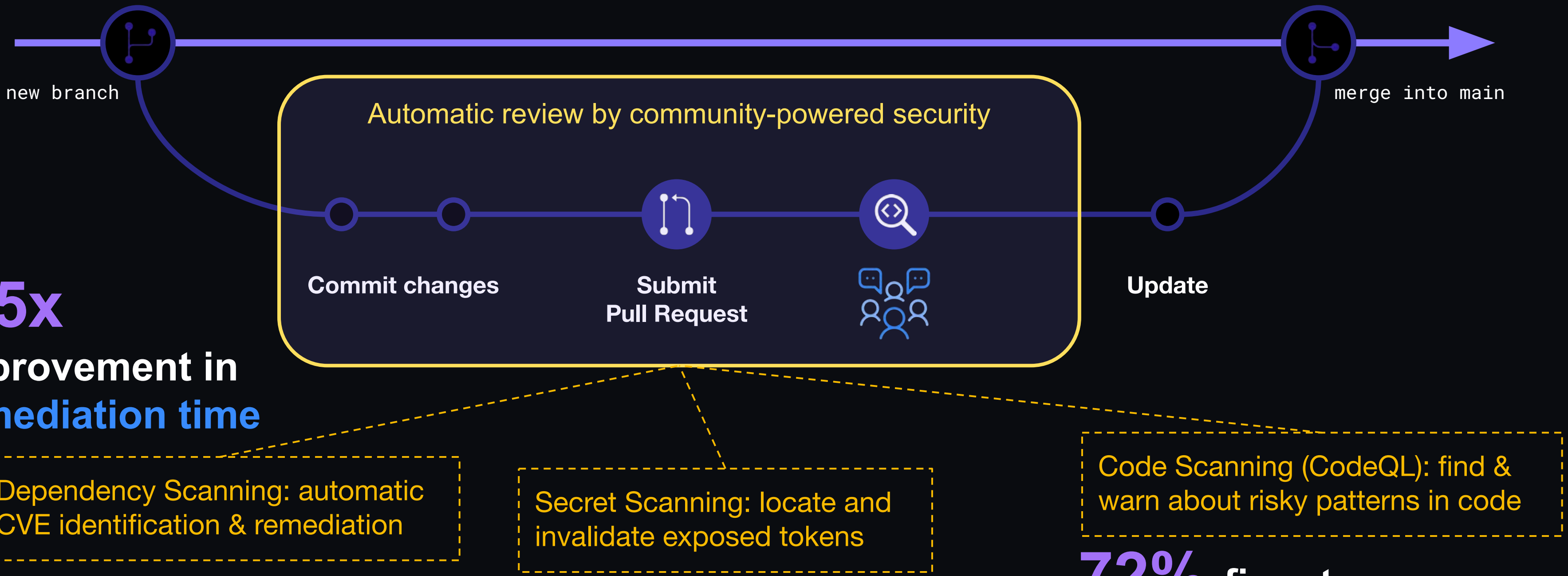
Code Scanning (CodeQL): find & warn about risky patterns in code

72% fix rate on
potential vulnerabilities

973x
More frequent deployments

6570x
Faster commit to deploy

2604x
Faster incident recovery



Dependency Scanning: automatic CVE identification & remediation

Secret Scanning: locate and invalidate exposed tokens

Code Scanning (CodeQL): find & warn about risky patterns in code

4.5x
improvement in
remediation time

Blocked at push
+ historic remediation

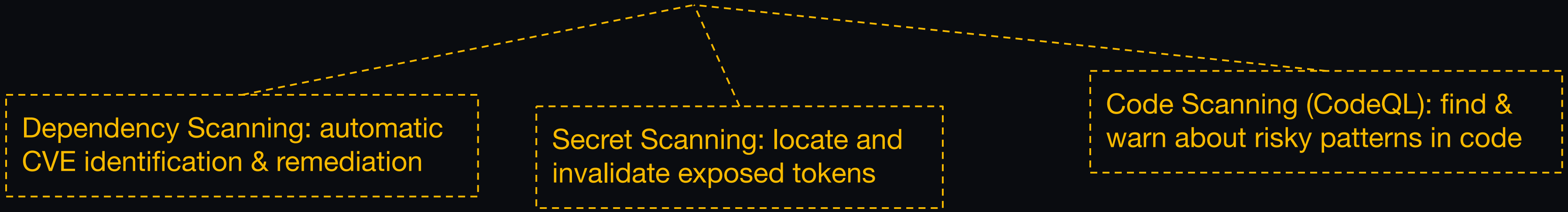
72% fix rate on
potential vulnerabilities

973x
More frequent deployments

6570x
Faster commit to deploy

2604x
Faster incident recovery

github.com/features/security



Dependency Scanning: automatic CVE identification & remediation

Secret Scanning: locate and invalidate exposed tokens

Code Scanning (CodeQL): find & warn about risky patterns in code