



SPS COMMERCE



# BEYOND SOURCE CONTROL LEVELING UP WITH THE GITHUB TOOLCHAIN

"A YEAR FROM NOW YOU WILL WISH YOU HAD  
STARTED TODAY." (KAREN LAMB)

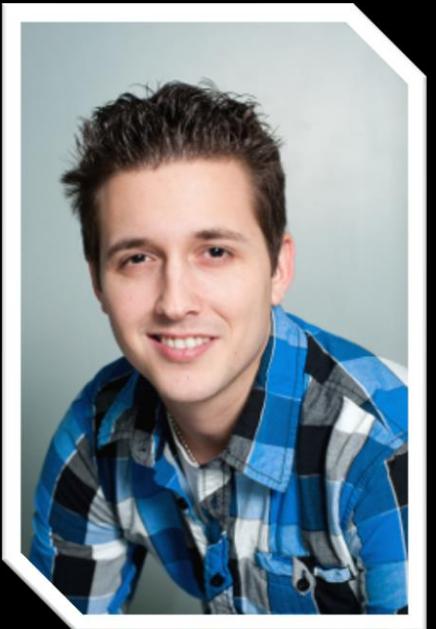


## Sponsors

accenture  
<dev>pro

## Community Sponsor

SGI



# TRAVIS GOSELIN

DISTINGUISHED SOFTWARE ENGINEER

DEVELOPER EXPERIENCE

[travisgosselin.com](http://travisgosselin.com)

[linkedin.com/in/travisgosselin](https://linkedin.com/in/travisgosselin)

@travisjgosselin



## SPS COMMERCE

INFINITE RETAIL POWER™

The screenshot displays the SPS Commerce platform's dashboard. At the top, there are four summary cards: 'Pending Partner Acknowledgement' (13), 'New Orders' (218), 'Errors' (21), and 'Ready for Change Acknowledgement' (59). Below these are sections for 'Open Orders' and 'Orders Missing a Shipment'. The 'Open Orders' table lists various trading partners with their order status and amounts. To the right, a 'RECENT ACTIVITY' sidebar shows a log of events from April 19 and 20, such as new orders and vendor compliance updates.

Date	Order #	Trading Partner	Status	Order Amount	Alert
Mar 7	N05504432-45	Dick's Sporting Goods	In Process	\$10,677.98	1
Mar 14	9000-00042618	Apex Sports	In Process	\$9,013.27	1
Mar 21	00007-655543	Walmart	In Process	\$22,996.71	
Mar 23	P00131866	Cabela's	In Process	\$11,901.01	1
Mar 29	G00009114	Champ's Sports	In Process	\$971.83	
Mar 30	O103064198	Finish Line	In Process	\$1,865.31	
Mar 30	Q101-044-45	Foot Locker	In Process	\$2,113.79	1
Mar 31	00001-77614	Gander Mountain	In Process	\$5,498.23	
Apr 5	B005-88760004	Bass Pro Shops	New	\$5,119.66	
Apr 11	0000119-887	Mills Fleet Farm	New	\$782.19	

"

Developer Experience is the activity of studying, improving and optimizing how developers get their work done.

"

[theappslab.com](http://theappslab.com) (2017)

# DEVELOPER EXPERIENCE

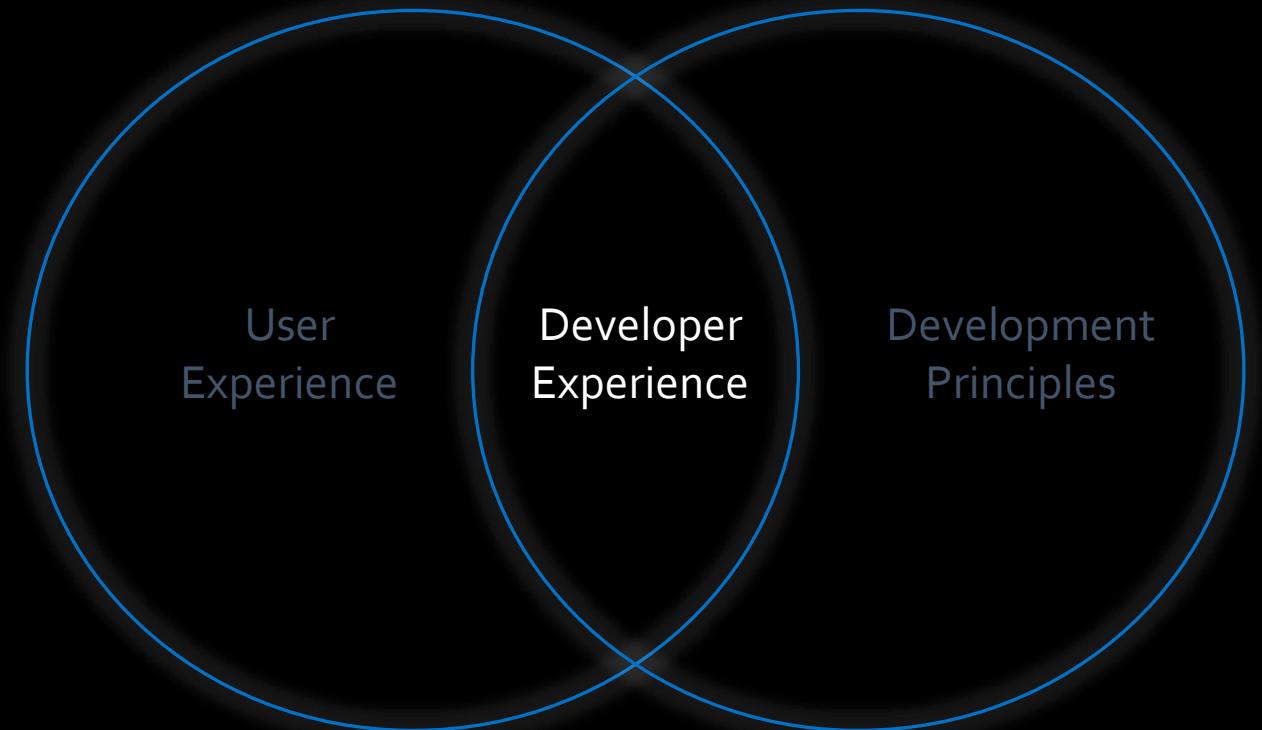
WHAT IS THAT...EXACTLY?

"

Developers work in rainforests, not planned gardens.

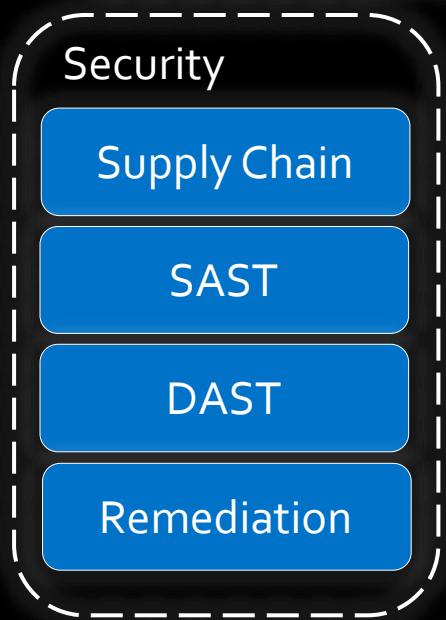
"

[a16z.com](http://a16z.com)



# CODING REALITY

We Need Help



Writing New or  
Updating Existing  
Coding



**Developers Code (Avg):  
52 min / Day**



Code time is often undervalued, continually interrupted, and almost wholly unmeasured.



Mason Mclead, CTO, Software.com

**Improve Daily Work**



**Fix Bottlenecks**

**More Automation**

**Reduce Feedback Cycle Duration**

**Codify Best Practices**

**Effective Documentation**

**Streamline Collaboration**

2008

Your Dashboard — GitHub

<https://github.com/> RSS

Apple (137) Amazon eBay Yahoo! News (1173)

Your Dashboard — GitHub

github

News Feed

for you | from you

emkay started watching bus-scheme 16 minutes ago  
bus-scheme is at technomancy/bus-scheme

defunkt started watching github-extras 31 minutes ago  
github-extras is at mojombo/github-extras

pjhyett started watching github-extras 31 minutes ago  
github-extras is at mojombo/github-extras

rubbish started watching grit about 1 hour ago  
grit is at mojombo/grit

rubbish started watching grit about 1 hour ago  
grit is at mojombo/grit

mojombo

account | profile | help | log out

Repositories

Your Repositories (create a new one)

all | public | private | sources | forks

chronic

fixture-scenarios

github-extras

glowstick

god

grit

vanhelsing

yaws

Watched Repositories

defunkt/github-extras

GIT Repository Hosting: No Longer a Pain in the Ass. Finally, a code repository that works as well as you do.

2011



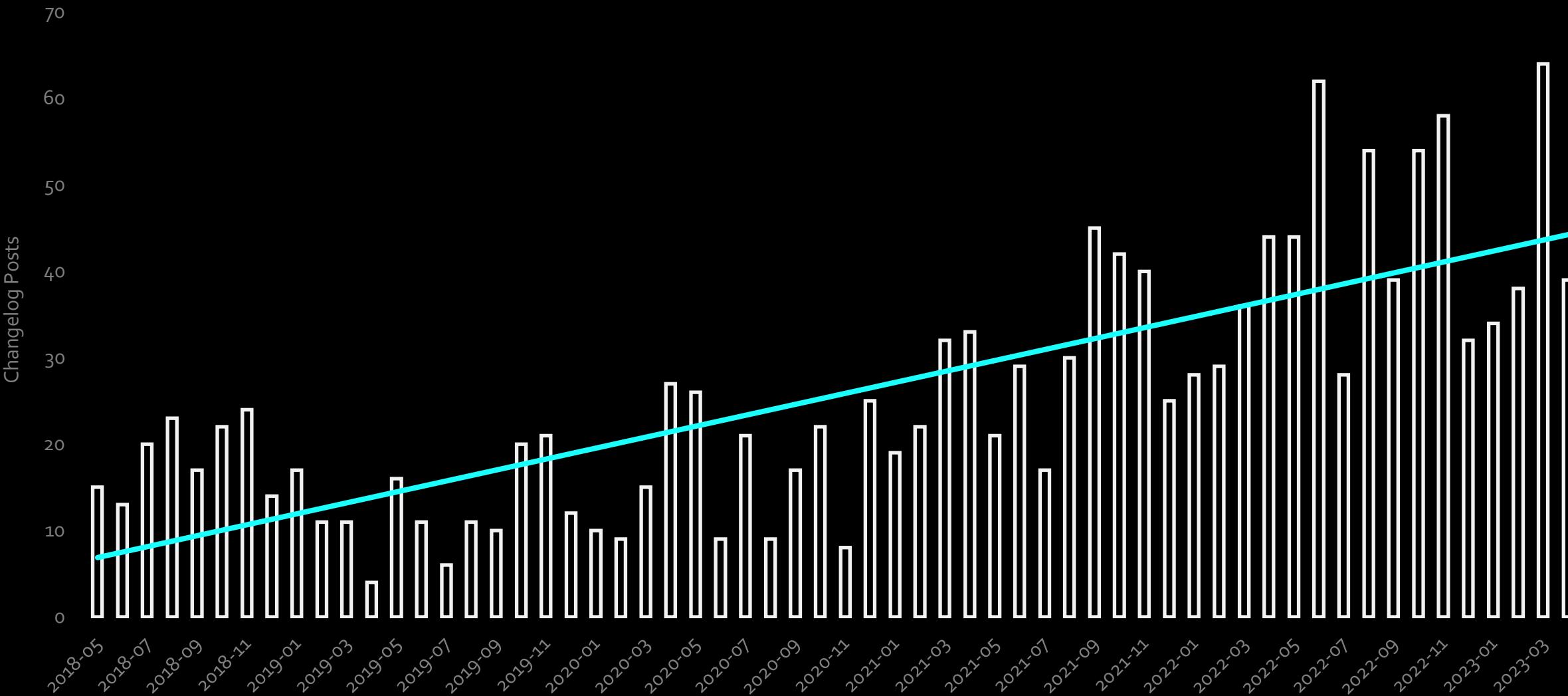
GitHub

Now The complete developer platform to build, scale, and deliver secure software.

We focus on lowering the barriers of collaboration by building powerful features into our products that make it easier to contribute

# GITHUB FEATURE RELEASES

Features Released Per Month



# GITHUB PLATFORM

Maximizing Developer Productivity

Core  
GitHub  
Features

1. Pull Requests

2. Dependabot

3. Advanced Security

4. Copilot

5. Pages

6. Discussions

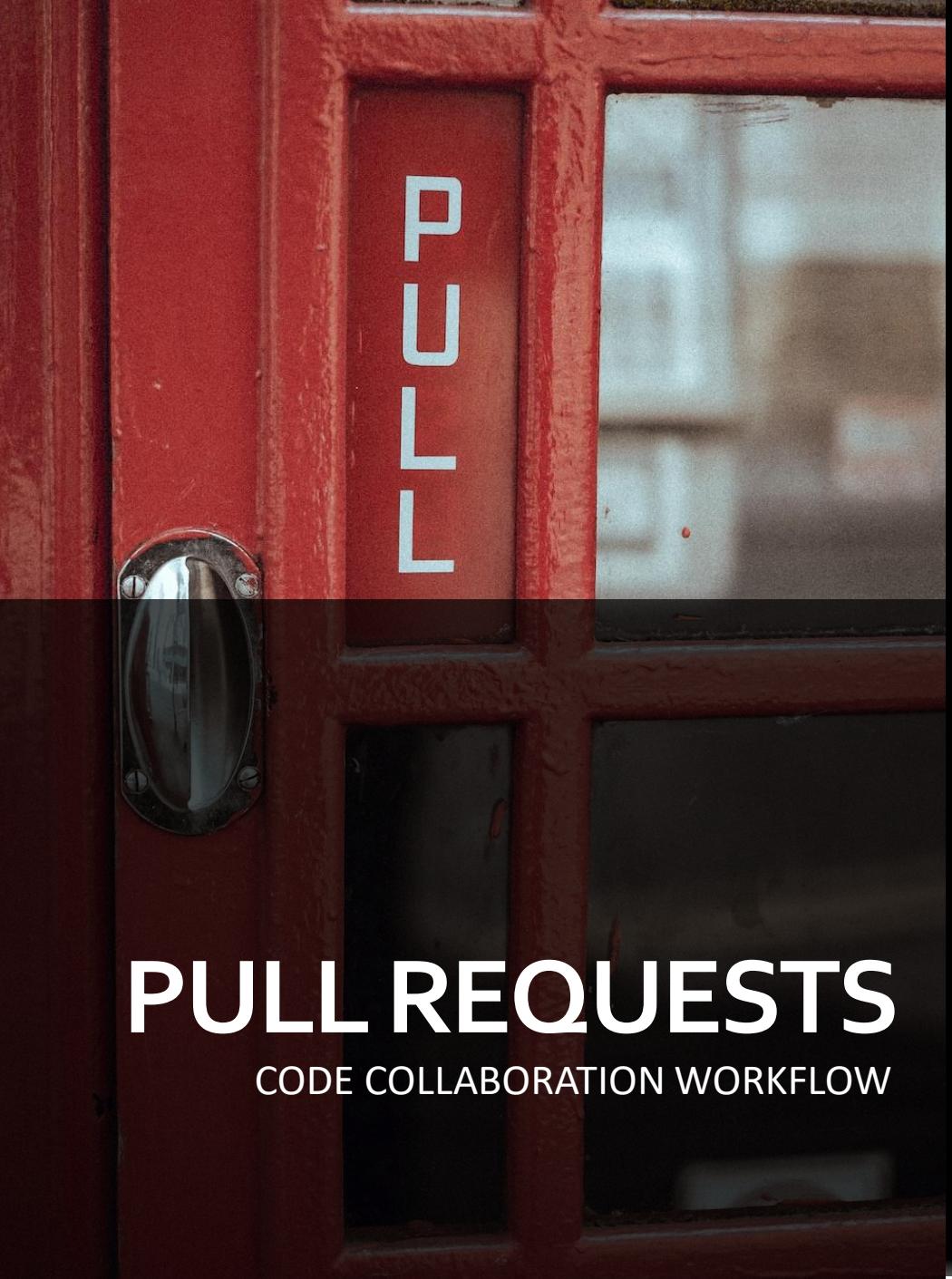
7. Packages

8. Codespaces



# PULL REQUESTS

## CODE COLLABORATION WORKFLOW

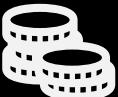


“ Pull requests let you tell others about changes you've pushed to a branch in a repository on GitHub. ”

[docs.github.com](https://docs.github.com)



Branch  
Protection



Rules



Merge Queues



*Why are  
they not called  
“Push  
Requests”*

# PULL REQUESTS

## Branch protection rule

Branch name pattern \*

main

Applies to 1 branch

main

Enforce certain workflows for one or more branches, highly integrated with Pull Requests

The diagram consists of two purple circles connected by a horizontal arrow pointing from left to right. The left circle contains the text '3 Options' above a green button labeled '2018'. The right circle contains the text '20 Options' above a green button labeled 'Now'. A blue callout box is positioned above the right circle, containing the text 'Enforce certain workflows for one or more branches, highly integrated with Pull Requests'.

2018	Now
3 Options	20 Options



# PULL REQUESTS

## Branch Protection Rules

### **Require a pull request before merging**

When enabled, all commits must be made to a non-protected branch and submitted via a pull request before they can be merged into a branch that matches this rule.

### **Require approvals**

When enabled, pull requests targeting a matching branch require a number of approvals and no changes requested before they can be merged.

Required number of approvals before merging: 1 ▾

### **Dismiss stale pull request approvals when new commits are pushed**

New reviewable commits pushed to a matching branch will dismiss pull request review approvals.

### **Require review from Code Owners**

Require an approved review in pull requests including files with a designated code owner.

### **Restrict who can dismiss pull request reviews**

Specify people, teams, or apps allowed to dismiss pull request reviews.

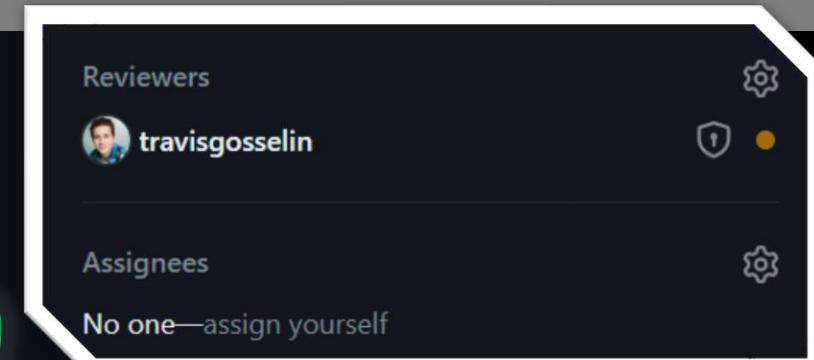
### **Allow specified actors to bypass required pull requests**

Specify people, teams, or apps who are allowed to bypass required pull requests.

### **Require approval of the most recent reviewable push**

Whether the most recent reviewable push must be approved by someone other than the person who pushed it.

```
-- .github/CODEOWNERS
*
file.js          @user1
/src/module-a/   @user2
/src/module-b/   @team1
```



# PULL REQUESTS

## Rulesets

Rulesets help you to control how people can interact with branches and tags in a repository.

docs.github.com



The image shows the GitHub Rulesets interface for a repository named 'main-branch-protection'. The left sidebar lists various settings like General, Access, Collaborators and teams, Team and member roles, Code and automation, Branches, Tags, Rules (which is selected and highlighted with a green box), Rulesets, and Insights. The main panel shows the 'General' tab with the rule name 'main-branch-protection', an 'Active' enforcement status, and a 'Not permitted' bypass mode. A note below says 'Determines who can bypass this ruleset.' At the bottom, it says 'Applies to 1 target: main'.

Branch protections

**Restrict creations**  
Only allow users with bypass permission to create matching refs.

**Restrict updates**  
Only allow users with bypass permission to update matching refs.

**Restrict deletions**  
Only allow users with bypass permissions to delete matching refs.

**Require linear history**  
Prevent merge commits from being pushed to matching branches.

**Require deployments to succeed before merging**  
Choose which environments must be successfully deployed to before branches can be merged into a branch that matches this rule.

**Require signed commits**  
Commits pushed to matching branches must have verified signatures.

**Require a pull request before merging**  
Require all commits be made to a non-target branch and submitted via a pull request before they can be merged.

**Additional settings**

**Require status checks to pass before merging**  
Choose which status checks must pass before branches can be merged into a branch that matches this rule. When enabled, commits must first be pushed to another branch, then merged or pushed directly to a branch that matches this rule after status checks have passed.

**Additional settings**

**Block force pushes**  
Prevent users with push access from force pushing to branches.

# PULL REQUESTS

Rulesets vs Branch Protection

Rule Layering

Ruleset Status

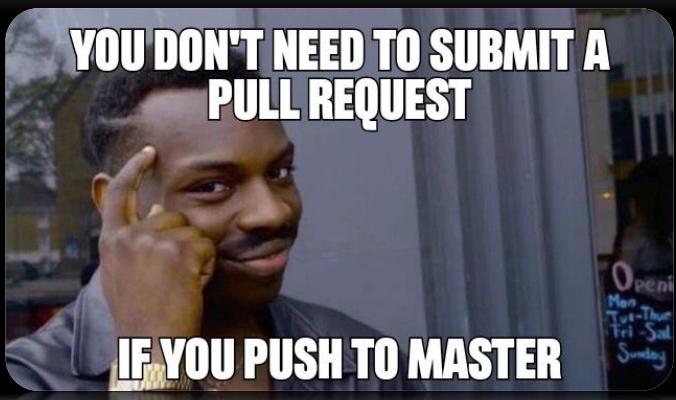
Ruleset Visibility

Restrict Creation

Branches or Tags

Bypass via GitHub App

Simpler UI / Identify Targets



The screenshot shows the GitHub Rulesets and Branch Protection interface. At the top, there's a list of branches: 'feature/doc-update' (Updated 1 hour ago by travisgosselin), 'codeql-pr-demo' (Updated last month by travisgosselin), and 'feature/api-spec-validation' (Updated 2 months ago by travisgosselin). Below this, the 'Rulesets' section shows two active rulesets: 'branching-naming-scheme' (Active, 2 rules targeting 2 branches) and 'main-branch-protection' (Active, 6 rules targeting 1 branch). A green box highlights the shield icon next to the first ruleset. A purple arrow points from this icon to the 'Branch protections' section of a detailed view of the 'main-branch-protection' ruleset. This detailed view includes sections for 'Target branches' (listing 'feature/\*\*/\*' and 'main'), 'Branch protections' (with 'Restrict creation' checked), and a note stating 'Applies to 2 targets including codeql-pr-demo, and main.' A green box also highlights this note. A white box highlights the 'main' branch under 'Target branches'. A purple arrow points from the 'Branch protections' section back up to the main interface. On the right side of the interface, there are buttons for 'New branch ruleset' and 'New tag ruleset'.

# PULL REQUESTS

## Rulesets in the Enterprise

### Metadata Restrictions

#### Metadata restrictions

Commit message must start with a matching pattern **TICKET-ID -**

Committer email must contain a matching pattern **test@test.com**

Commit Patterns / Enforce Ticket Requirements

Enforce Dynamic Users (**\*@org.com**)

### Insights (Evaluations)

#### Rule Insights Beta

All Rulesets All branches All users Last 24 hours

Activity on Jun 9, 2023

##### Update Dockerfile

travisgosselin pushed 805daf1..05ed124 to main 2 hours ago

##### Update Dockerfile

travisgosselin pushed 805d...

##### Update Dockerfile

travisgosselin pushed 805d...

Some rules did not pass

Branch Protection 2 rules failed

Require merge queue

Require a pull request before merging (#299)

At least 1 approving review is required by reviewers with write access.

Block force pushes



### Organizational Rulesets

#### Target repositories

No repository targets have been added yet

Repository targeting determines which repositories will be protected by this ruleset. Use inclusion patterns to expand repositories under this ruleset. Use exclusion patterns to exclude repositories.

Add a target

+ Include all repositories

Target by inclusion or exclusion pattern

+ Include by pattern

- Exclude by pattern

Prevent renaming of target repositories

When checked, target repositories can only be renamed by those with bypass permission.

Org Level Branch Protection

Auditor Benefits (Require Approver)

Codifying Best Practices

# PULL REQUESTS

## Merge Queues: Branch Protection

### **Require merge queue** Beta

Merges to matching branches must be performed via a merge queue.

Make sure to configure your CI to build branches created by the queue.

#### **Merge method**

Method to use when merging changes from queued pull requests.

Method: Squash and merge ▾

#### **Build concurrency**

Limit the number of queued pull requests building at the same time.

Maximum pull requests to build:

5

#### **Merge limits**

Limit the number of pull requests merged into the protected branch in a single merge operation.

Minimum pull requests to merge:

1

or after

5

minutes

Maximum pull requests to merge:

5

Only merge non-failing pull requests

#### **Status check timeout**

Time (in minutes) a required status check must report a conclusion within to not be considered failed.

Consider check failed after: **60** minutes

Based on enabled commit types in settings

Don't starve CI agents with Merge Queues

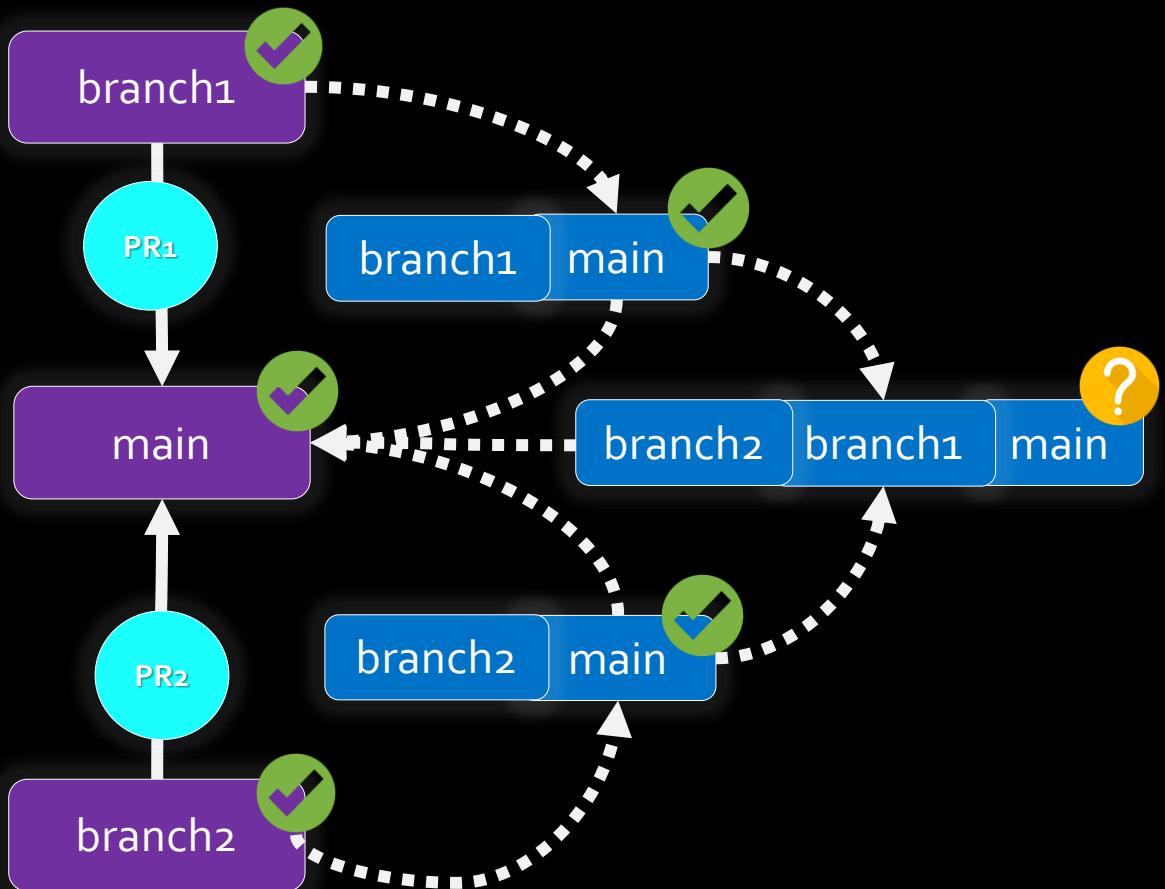
How to batch the incoming Pull Requests

Why would you disable this?

# PULL REQUESTS

Merge Queues: Why?

Semantic Conflicts

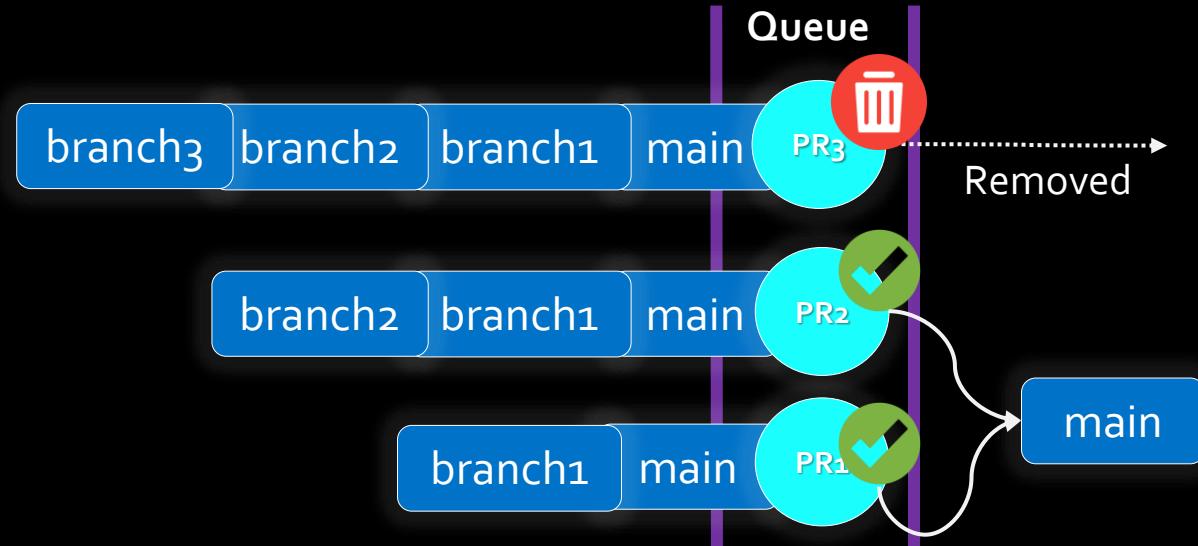


Solution 1: Require Up To Date Branches

**Require branches to be up to date before merging**

This ensures pull requests targeting a matching branch have been tested at least one status check is enabled (see below).

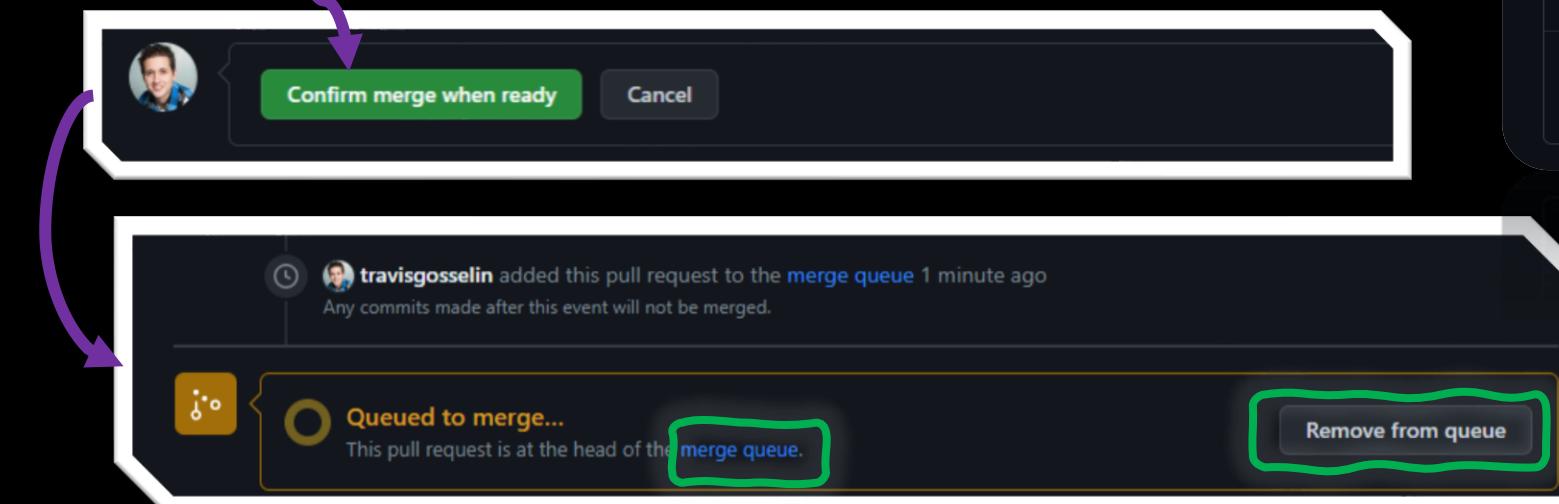
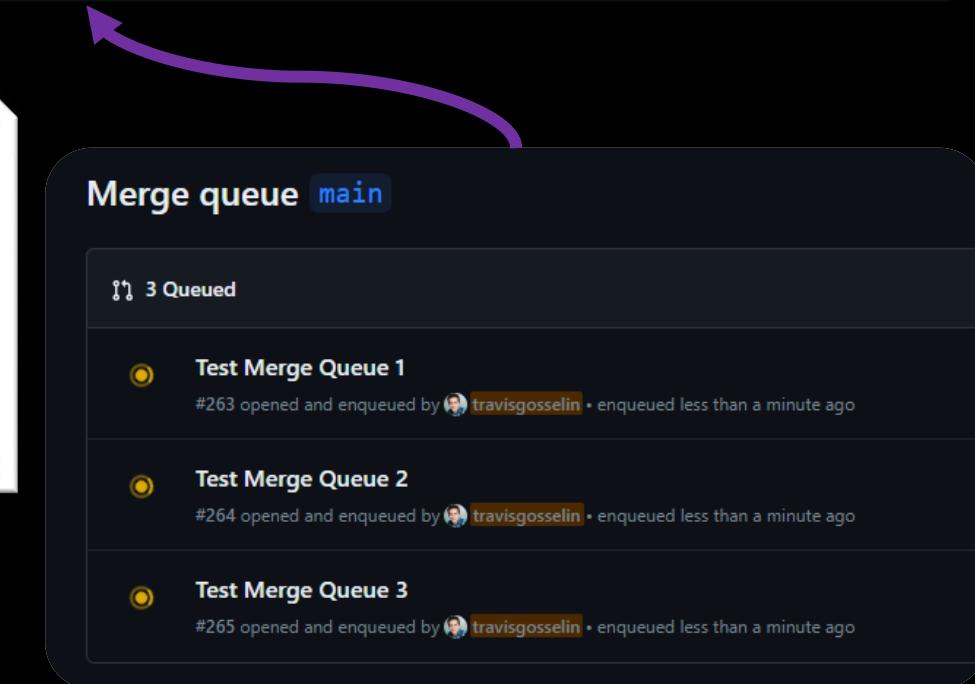
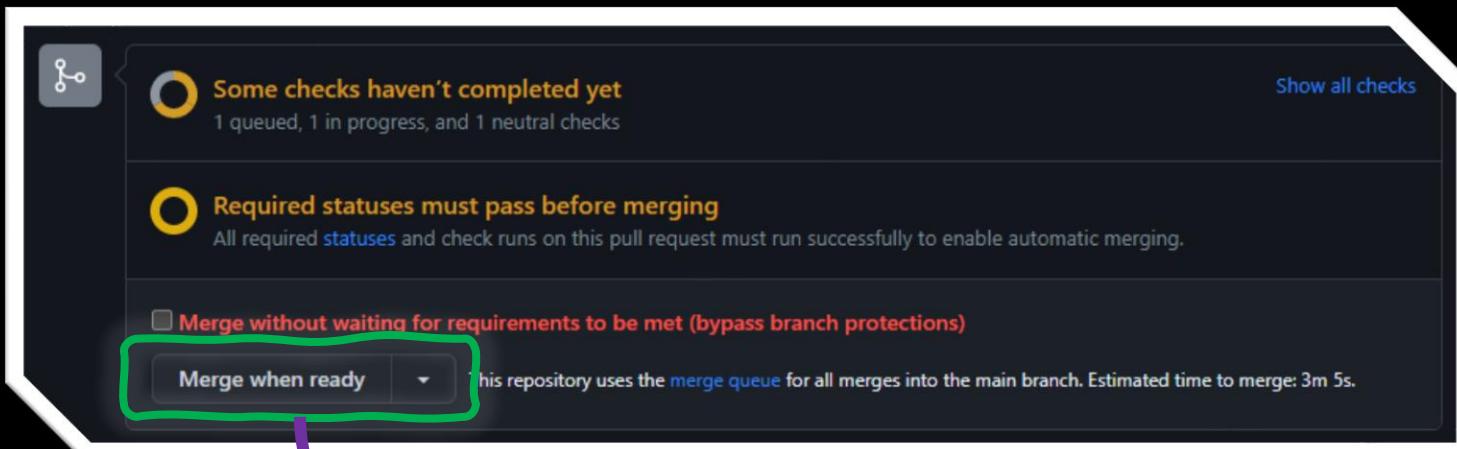
Solution 2: Merge Queue



# PULL REQUESTS

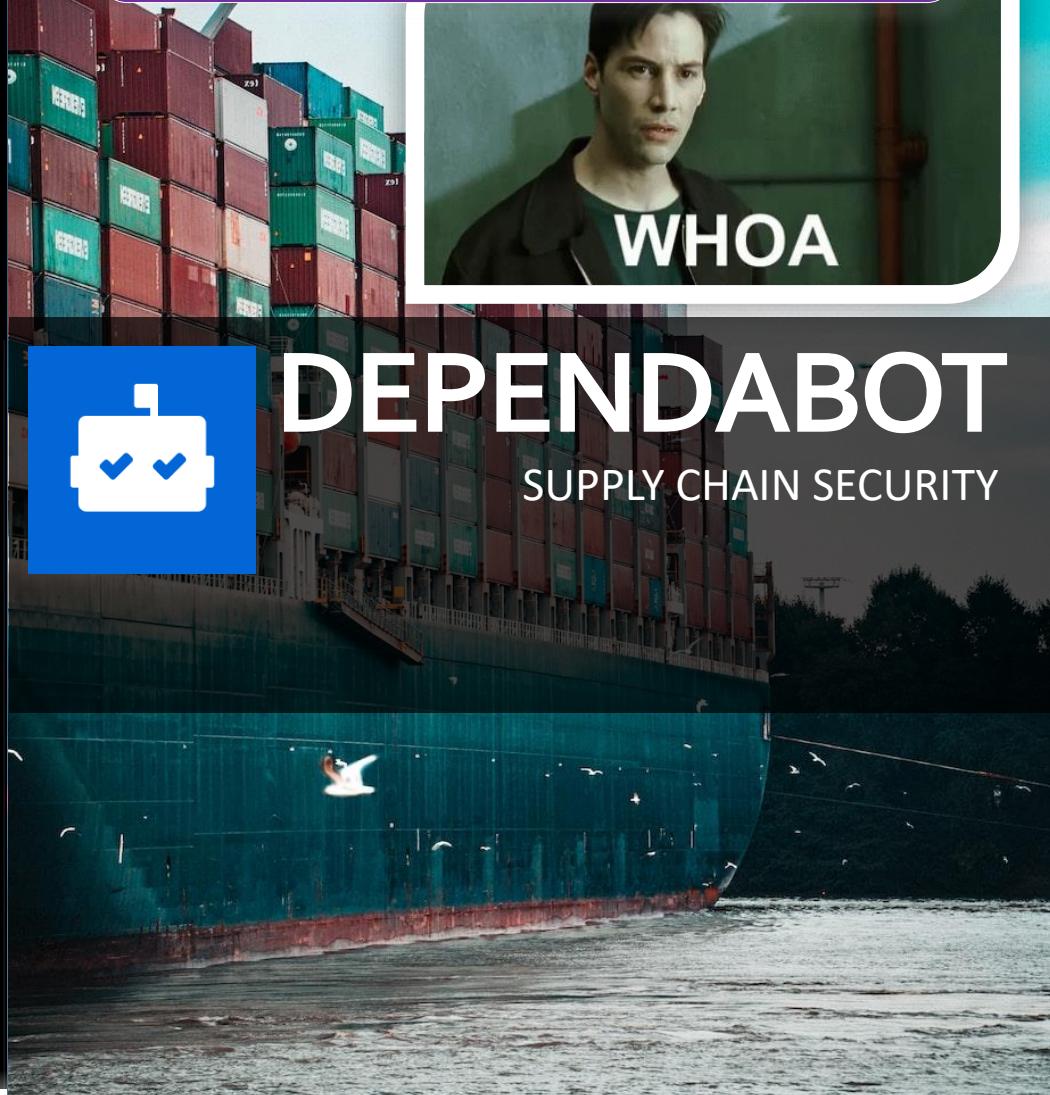
Merge Queues: GitHub

gh\_READONLY\_QUEUE/{target-branch}/pr-{pr-number}-{id}  
gh\_READONLY\_QUEUE/main/pr-238-36bof88c80a341d4c9894fdf6b7eba6ee668f28a  
gh\_READONLY\_QUEUE/main/\*



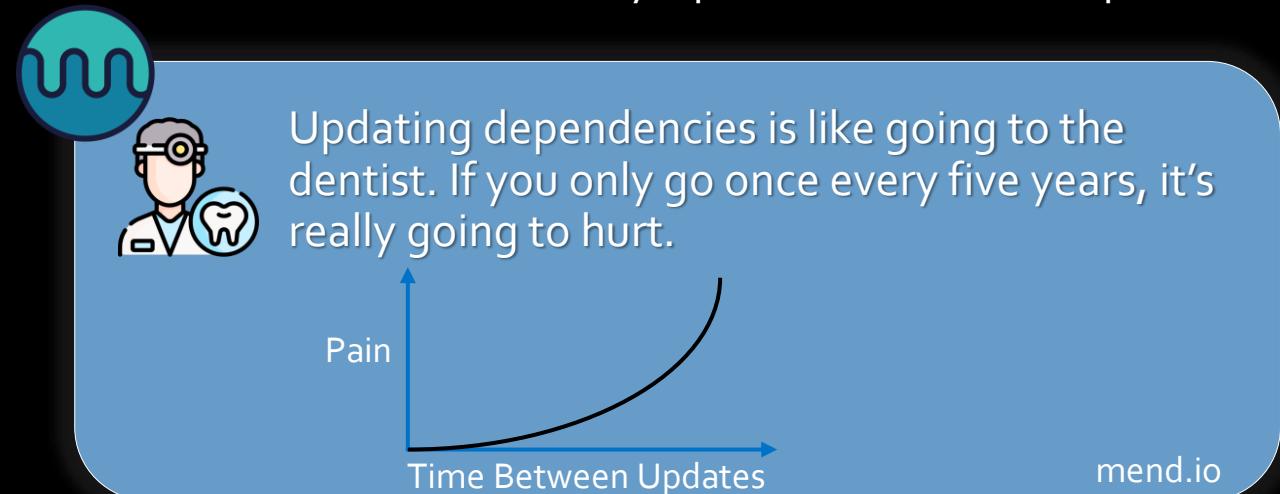


2021 Over 90% of CVEs not present  
in most Recent Dependency Versions



“ Monitor vulnerabilities in dependencies used in your project and keep your dependencies up-to-date with Dependabot.

”



# DEPENDABOT

## Overview

The screenshot shows the GitHub Dependabot settings interface. On the left, there's a sidebar with navigation links like General, Access, Collaborators and teams, Team and member roles, Code and automation (Branches, Tags, Rules, Actions, Webhooks, Environments, Codespaces, Pages), Security, and Code security and analysis (which is highlighted with a green box). The main area has tabs for Insights and Settings. Under Insights, there are sections for Pulse, Contributors, Community, Traffic, Commits, Code frequency, Dependency graph (which is highlighted with a green box), Network, Forks, and a search bar. The Dependency graph section lists dependencies: Microsoft.Extensions.Http.Polly 6.0.15 (detected on Apr 03, 2023), refit 6.3.2 (detected on Apr 03, 2023), and Refit.HttpClientFactory 6.3.2 (detected on Apr 03, 2023). There are also sections for Dependabot alerts (highlighted with a green box), Dependabot security updates (highlighted with a green box), and Dependabot version updates (highlighted with a green box). Each section includes a 'Disable' button.

**Code security and analysis**

**Dependency graph**  
Understand your dependencies.

**Dependabot**  
Keep your dependencies secure and up-to-date. [Learn more about Dependabot](#).

**Dependabot alerts**  
Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. [Configure alert notifications](#).

**Dependabot security updates**  
Allow Dependabot to open pull requests automatically to resolve Dependabot alerts.

**Dependabot version updates**  
Allow Dependabot to open pull requests automatically to keep your dependencies up-to-date when new versions are available. [Learn more about configuring a dependabot.yml file](#).

# DEPENDABOT

## Alerts & Security Updates

Security 118   Insights   Settings

Overview   Dependabot   Reporting   Policy   Advisories

Vulnerability alerts

Dependabot 118   Secret scanning

Dependabot alerts / #650

Spring Framework is vulnerable to security bypass via mvcRequestMatcher pattern mismatch #650

Open   Opened 3 weeks ago on org.springframework:spring (Maven) · pom.xml

Upgrade org.springframework:spring to fix 1 Dependabot alert in pom.xml

Upgrade org.springframework:spring to version 5.3.26 or later. For example:

```
<dependency>
  <groupId>org.springframework</groupId>
  <artifactId>spring</artifactId>
  <version>[5.3.26,)</version>
</dependency>
```

Create Dependabot security update

Package	Affected versions	Patched version
org.springframework:spring (Maven)	>= 5.3.0, < 5.3.26	5.3.26

Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "\*" as a pattern in Spring Security configuration with the mvcRequestMatcher creates a mismatch in pattern matching between Spring Security and Spring MVC, and

Dependency graph  
Understand your dependencies.

Automatically enable for new private repositories

Disable all   Enable all

Dependabot  
Keep your dependencies secure and up-to-date. [Learn more about Dependabot](#).

Dependabot alerts  
Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. [Configure alert notifications](#).

Automatically enable for new repositories

Disable all   Enable all

Dependabot security updates  
Allow Dependabot to open pull requests automatically to resolve Dependabot alerts.

Automatically enable for new repositories

Disable all   Enable all

Dependabot

99% of repositories protected

Alerts  
3,744 enabled   26 not enabled

Security updates  
143 enabled   3,627 not enabled



## Pull Request Build Triggers

Dismiss alert ▾

Select a reason to dismiss

- A fix has already been started
- No bandwidth to fix this
- Risk is tolerable to this project
- This alert is inaccurate or incorrect
- Vulnerable code is not actually used

Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Tags

Direct dependency   Patch available

# DEPENDABOT

## Version Updates

### Supported Ecosystems

gomod maven gradle npm

nuget pip elm ...

docker terraform  
github actions git submodule

helm? [dependabot/dependabot-core/issues/2237](https://github.com/dependabot/dependabot-core/issues/2237)

### Private Feed Configuration with Secrets

### Update Schedule

### Metadata Configuration

### Behavior Configuration

Dependabot version updates are automated pull requests that keep your dependencies updated, even when they don't have any vulnerabilities.

[docs.github.com](https://docs.github.com)

**2023** 83% of security teams don't have access to a fully accurate SBOM in real time!



The screenshot shows the Dependabot interface with two main sections. The top section displays a dependency graph for a Microsoft.AspNetCore project, with tabs for Dependencies, Dependents, and Dependabot. The Dependabot tab is active, showing a status message: "src/Spsc.AspNetCore.Demo.Web/Spsc.AspNetCore.Demo.Web.csproj ... Last checked last week". The bottom section shows another dependency graph for a different project, with a "Check for updates" button highlighted with a green border. Below it is an "Update logs" section displaying command-line output for a proxy and updater process, including log entries like "proxy | 2023/04/21 19:18:56 proxy starting, commit: d7dc5b938d3a555f3a197631d3de2abe3853c50" and "updater | 2023-04-21T19:18:56.363985811 [649596265:main:WARN:src/devices/src/legacy/serial.rs:222] Detached the serial input due to peer close/error".

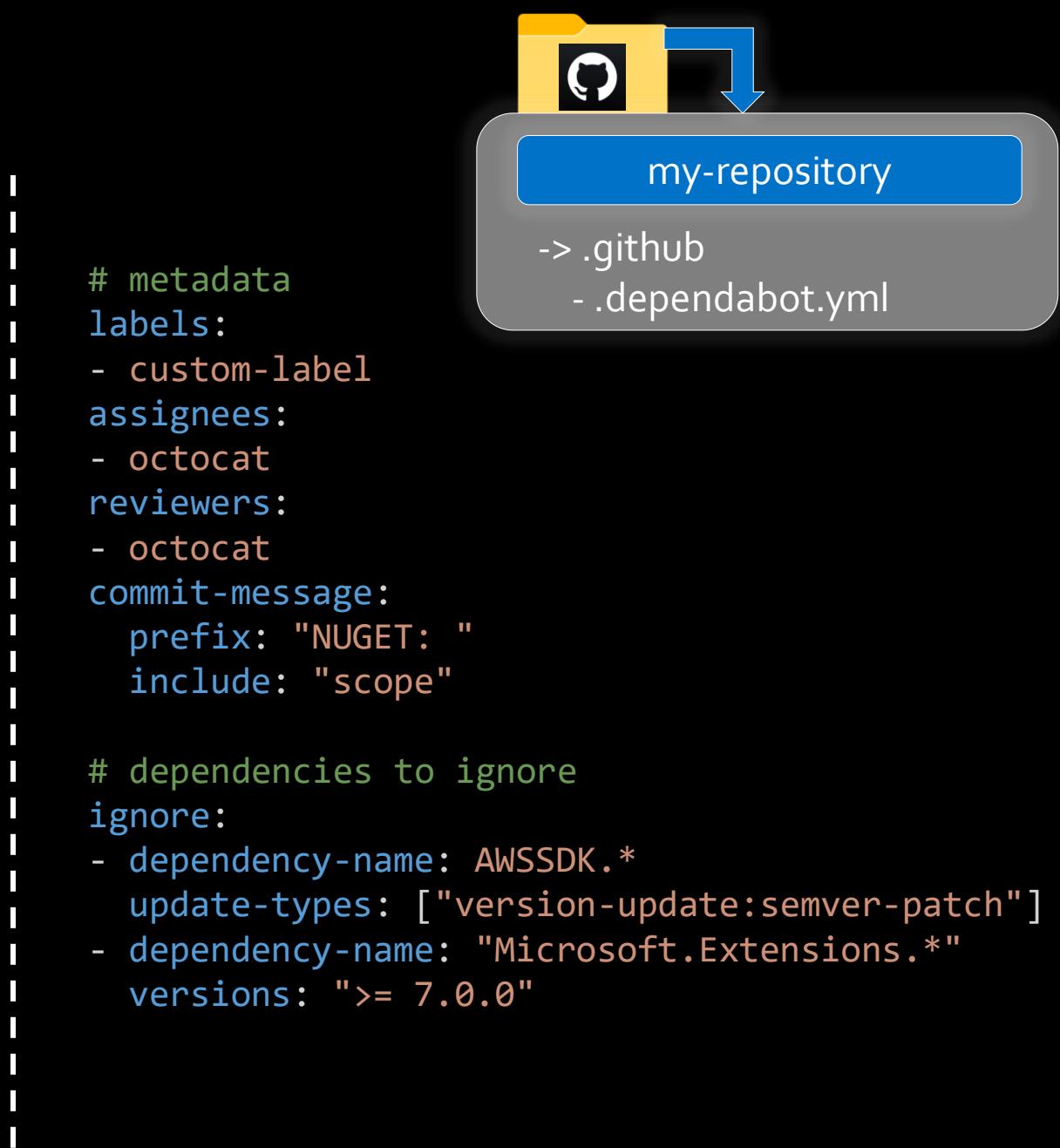
# DEPENDABOT

## Version Updates: Configuration

```
version: 2

registries:
  nuget-azure-devops:
    type: nuget-feed
    url: https://pkgs.dev.azure.com/index.json
    username: your-user
    password: ${{secrets.NUGET_TOKEN_V1}}

updates:
  # keep NUGET dependencies up to date
  - package-ecosystem: nuget
    directory: "/"
    registries:
      - nuget-azure-devops
    schedule: # set day, time, timezone, etc
      interval: daily # weekly / monthly
    open-pull-requests-limit: 10
```



# DEPENDABOT

Version Updates: Grouped Pull Requests

...

updates:

- package-ecosystem: nuget  
directory: "/"  
...

groups:

test-dependencies:

patterns:

- "MSTest.\*"
- "NSubstitute\*"

Custom Groups

exclude-patterns:

- "Other.\*"

Exclude Patterns

core-dependencies:

patterns:

- "Spac.\*"
- "Microsoft.Extensions.\*"
- "Microsoft.AspNetCore.\*"

aws:

patterns:

- "AWSSDK.\*"

Catch-All

groups:

all-dependencies:

patterns:

- "\*"

Dependency Types

groups:

production-dependencies:

dependency-type: "production"

development:

dependency-type: "development"

Update Types

groups:

angular:

patterns:

- "@angular\*"

update-types:

- "minor"
- "patch\*"

2020

29%

Shift towards consolidating security vendors due to operational inefficiencies!

2022

75%

# ADVANCED SECURITY

WHAT DO YOUR DEVSECOPS PRACTICES LOOK LIKE?

<https://www.dynatrace.com/monitoring/platform/application-security/>

CHAPTER 4

## Tool sprawl and team silos hinder DevSecOps practices

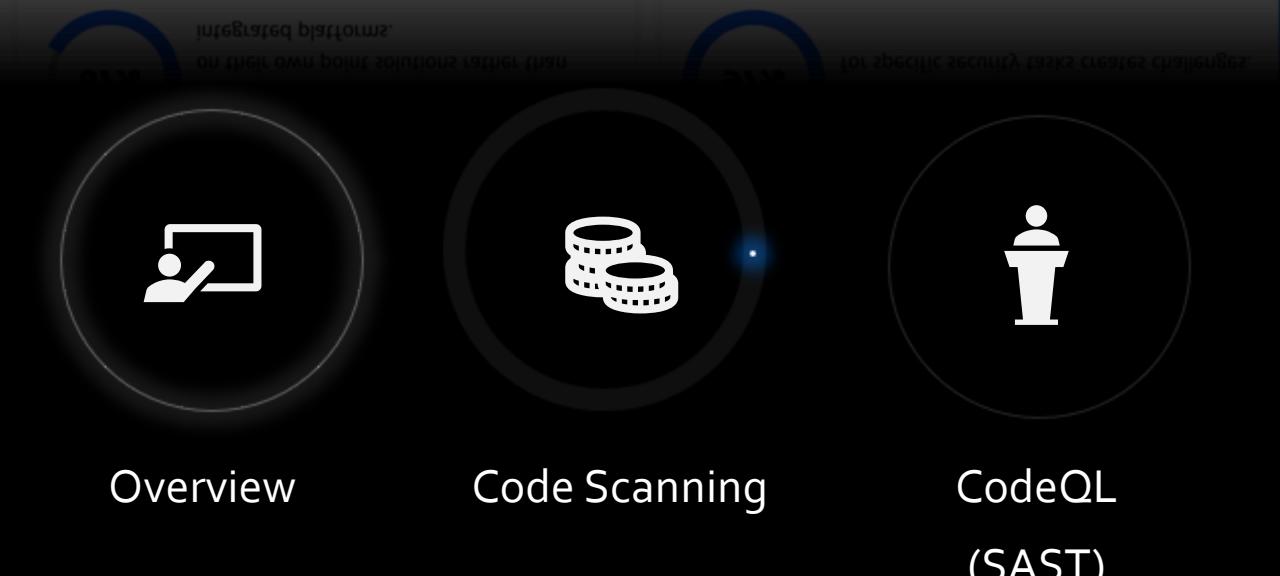
As organizations work to accelerate their transformation, they are increasingly embracing a more collaborative DevSecOps culture that encourages development, security, and operations teams to work together toward shared goals. However, entrenched preferences for specific point solutions within different teams hinder these efforts, resulting in silos and multiple versions of the truth. The convergence of observability and security analytics is critical to overcoming these challenges, by uniting teams around a single source of truth that supports DevSecOps automation.



of CISOs say development, security, and operations teams continue to rely on their own point solutions rather than integrated platforms.



of CISOs say the use of point solutions for specific security tasks creates challenges.



# ADVANCED SECURITY

## Overview



1 License Per User

1 License for Repository Active Committer (90 Days)

Security

**Code security and analysis**

Deploy keys

Secrets and variables

Integrations

GitHub Apps

Email notifications

Autolink references

## GitHub Advanced Security

GitHub Advanced Security features are billed per active committer in private and internal repositories. [Learn more about advanced security billing.](#)

**Code scanning**

Automatically detect common vulnerabilities and coding errors.

**Secret scanning**

Receive alerts on GitHub for detected secrets, keys, or other tokens.

 Push Protection Generally Available for Public Repos

17,000 Potential Credentials Blocked In 1-Year

**Disable**

**Disable**

# ADVANCED SECURITY

## Code Scanning

The screenshot shows the GitHub Code Scanning interface. On the left, there's a sidebar with sections for 'Code scanning' (highlighted), 'Tools' (CodeQL analysis and Other tools), and 'CodeQL analysis'. The main area displays a code alert titled 'Generic catch clause'.

**Code Scanning Alerts / #49**

**Generic catch clause**

**src/Spsc.AspNetCore.Demo.Web.Api/v1/ExamplesController.cs.cs:185**

```
182
183         return new Value() { Result = $"Success: { url } - { content }" };
184     }
185     catch (Exception ex)
186     {
187         return new Value() { Result = $"Fail: { ex.Message }" };
188     }
```

Generic catch clause.

CodeQL

```
189     }
190
191     /// <summary>
```

**Tool**: CodeQL    **Rule ID**: cs/catch-of-all-exceptions    **Query**: View source

Catching all exceptions with a generic catch clause may be overly broad. This can make errors harder to diagnose when exceptions are caught unintentionally.

Show more ▾

First detected in commit on Jun 24, 2022

Update dependencies / service template.

✓ df9c4b0

#50 closed as fixed 10 months ago • Detected by CodeQL in tests/Spsc.AspNetCore.Demo.Int.../TestHelper.cs:27 last year

**Select a reason to dismiss**

- Won't fix  
This alert is not relevant
- False positive  
This alert is not valid
- Used in tests  
This alert is not in production code

Tags: maintainability, reliability

Weaknesses: CWE-396

# ADVANCED SECURITY

## Code Scanning on Pull Requests

Top Challenge: Correlating alerts from different tools is labor-intensive, with many false positives.  
2023



**Protection rules**

**Pull request check failure**  
Define which code scanning alert severity should cause a pull request check to fail to analysis results uploaded via the API.

All checks have passed  
1 neutral and 6 successful checks

- sps-ref-dotnetcore-client — This check was skipped
- Code scanning results / CodeQL** Successful in 5s — 1 new alert
- sps-ref-dotnetcore-api Successful in 3m — Build #0.0.0-pr28

### CodeQL Example Issue #289

Open travisgosselin wants to merge 1 commit into main from codeql-pr-demo

Conversation 0 Commits 1 Checks 0 Files changed 1

github-code-scanning (bot) found potential problems 2 minutes ago

src/Spse.AspNetCore.Demo.Web/Api/v1/ExamplesController.cs.cs

```
... ... @@ -72,6 +72,8 @@  
72 72 // you can add key/value (string/object) to serialize and attach to contextual output  
73 73 // in xray and in serilog  
74 74 _contextLogger.AddMetadata("TheThing1", "It works!");  
75 +  
76 + var unusedVariable = "unused variable to detect in CodeQL scan";
```

⚠ Check warning

Code scanning / CodeQL

Useless assignment to local variable ⚠ Warning

This assignment to unusedVariable is useless, since its value is never read.

Show more details

Dismiss alert

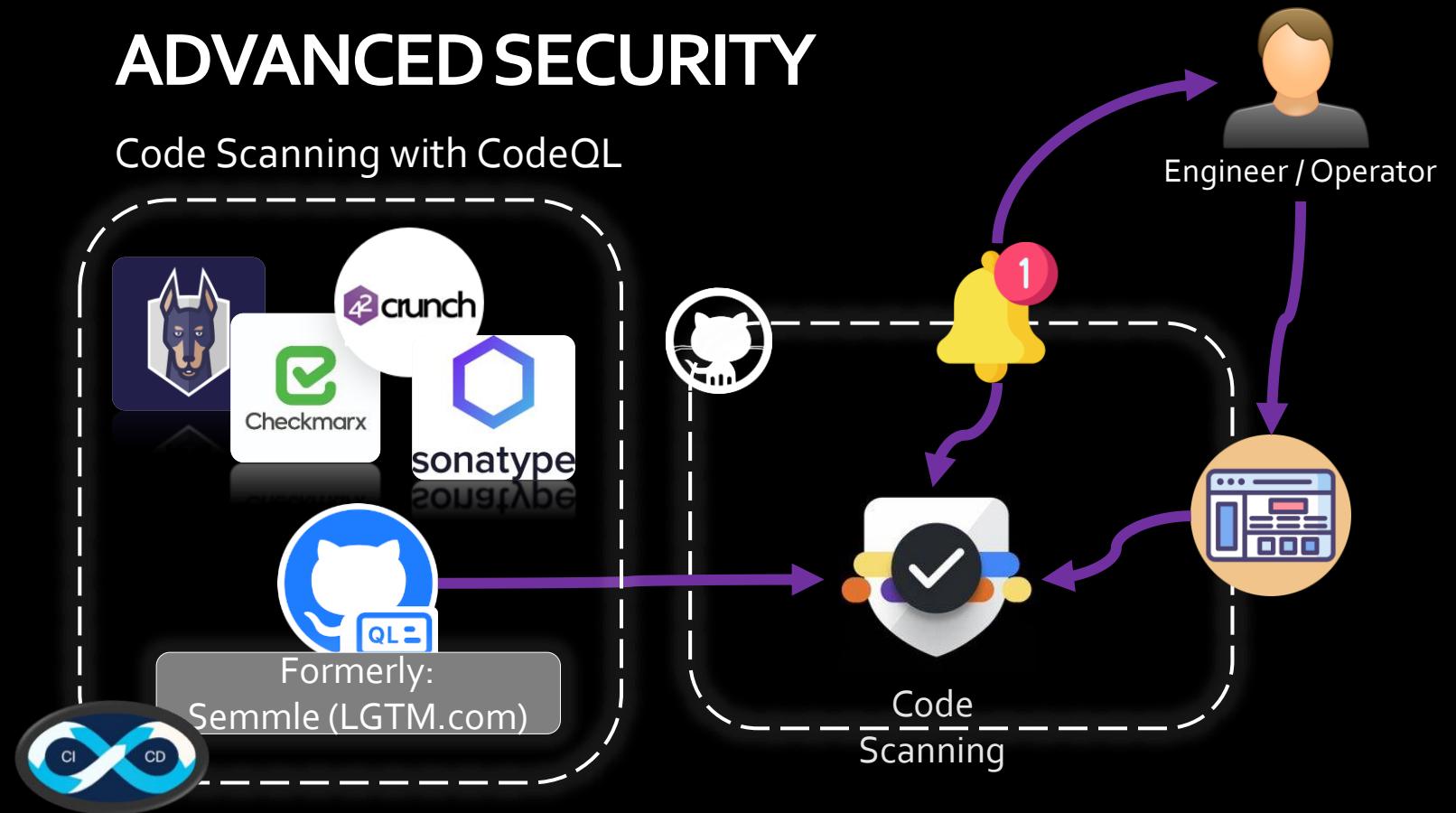
Reply...

“  
It makes no more sense to write code without code scanning tools than it does to write a paper without spell check.  
Mike Lyman (Synopsys)

page 40

# ADVANCED SECURITY

## Code Scanning with CodeQL

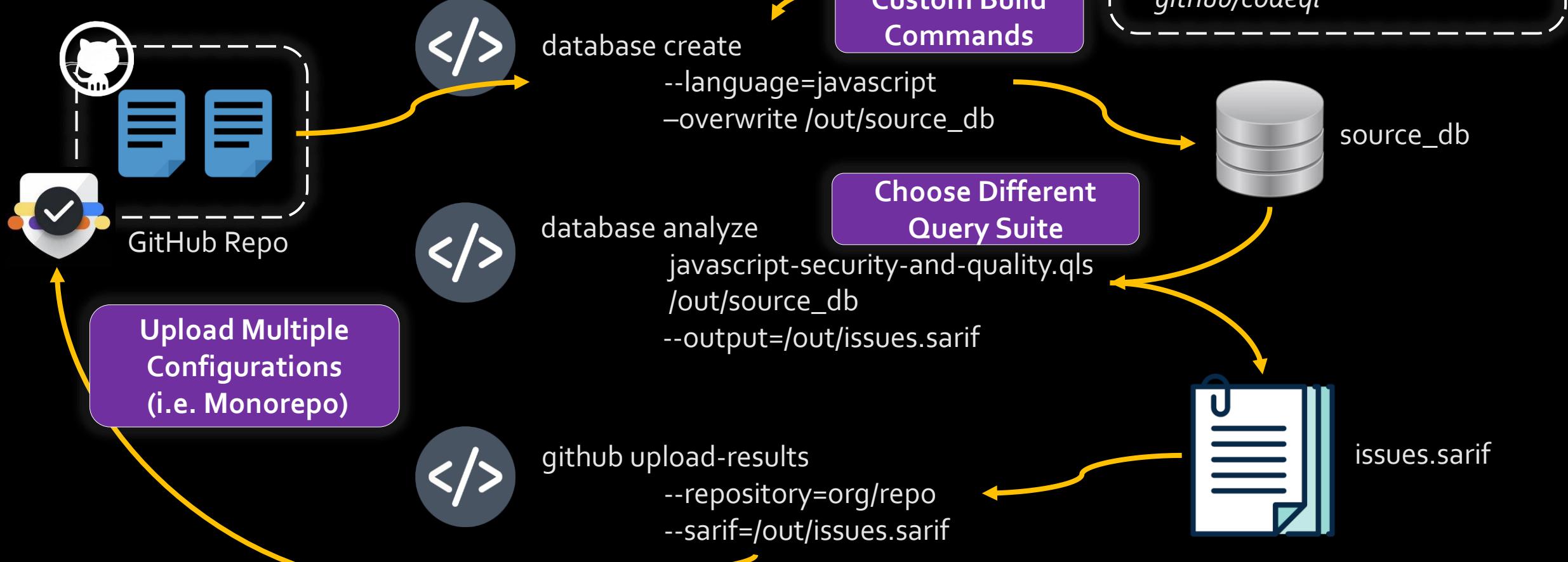


Screenshot of the GitHub Marketplace showing 67 workflows for Code Scanning:

- CodeQL Analysis** By GitHub: Security analysis from GitHub for C, C++, C#, Go, Java, JavaScript, TypeScript, Python, Ruby and Kotlin developers. **Configure** **Code scanning** ●
- Codacy Security Scan** By Codacy: Free, out-of-the-box, security analysis provided by multiple open source static analysis tools. **Configure** **Code scanning** ●
- Snyk Security** By Snyk: Detect vulnerabilities across your applications and infrastructure with the Snyk platform. **Configure** **Code scanning** ●
- Sysdig Inline Scan** By Sysdig: Performs analysis on locally built container image and posts the results in SARIF report. **Configure** **Code scanning** ●
- Checkmarx** By Checkmarx: Beat vulnerabilities with more secure code. Scan your code with Checkmarx One and see your results in the GitHub security tab. **Configure** **Code scanning** ●
- CxSAST** By Checkmarx: Scan your code with Checkmarx CxSAST and see your results in the GitHub security tab. **Configure** **Code scanning** ●

# ADVANCED SECURITY

CodeQL CLI



SARIF - Static Analysis Results Interchange Format  
Streamlines How Static Analysis Tools Share Results

**COPILOT**  
AI PAIR PROGRAMMER

2022

40% of code from users with Copilot is written by Copilot

Pushing for 80%

“ Trained on billions of lines of code, GitHub Copilot turns natural language prompts into coding suggestions across dozens of languages.

github.com

File Edit Selection View Go Run Terminal ... • app.js - copilot-test - Visual Studio Code [Administrator]

```
JS app.js
JS app.js
1 // calculate the number of days between two
2
3
```

Ln 2, Col 1 Spaces: 4 CRLF {} JavaScript ⚡ Prettier ⚡ [off] 🔍

# COPilot

## Overview

Comment-Based Prompt Engineering

Contextualized Code Suggestions

Focus on Solving Problems, Not Syntax

### IDE Support



### Language Support



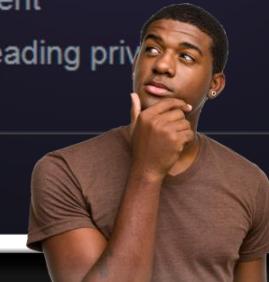
## For Individuals

- Plugs right into your editor
- Turns natural language prompts into code
- Offers multi-line function suggestions
- Speeds up test generation
- Blocks suggestions matching public code

## For Business

*Everything included in Copilot for Individuals, plus*

- Simple license management
- Organization-wide policy management
- Industry-leading pri



2022

Matthew Butterick



Open-Source Copyright  
Class Action Lawsuit

[GitHubCopilotInvestigation.com](http://GitHubCopilotInvestigation.com)

How is this Trained?

CoPilot is bold [and] innovative IMHO, but could have been equally transformative if they had obtained consent or respected the licenses — which would have been comparatively straightforward to achieve given their budget.

Alex Champandard (creative.ai Founder)

Copilot for Business won't retain, store or share code!

# COPilot

## Effectiveness

96%

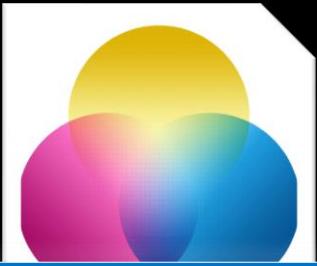
Say they are faster with repetitive tasks.

88%

Say they are more productive.

74%

Focus on more satisfying work.



Polyglot



Educational

“Use these tools wisely and be mindful of when to—and when not to—automate. For example, I can easily give ChatGPT an article and ask it to summarize the text for my notes. While this saves time, it robs me of the mental distillation of my thoughts (part of the learning process). As a knowledge worker who wishes to remain competitive for another couple of decades, thinking and learning are the most prized things I can do with my time.”

Michael Carducci

## Using GitHub Copilot Chat correlates with better code quality

85% of developers felt more confident in their code quality when authoring code with GitHub Copilot and GitHub Copilot Chat

85%

Code reviews were more actionable and completed 15% faster than without GitHub Copilot Chat

15%

88% of developers reported maintaining flow state with GitHub Copilot Chat

88%



# COPilot

Fails



Travis Gosselin @travisjgosselin · Nov 24, 2022

Loving GitHub Copilot.... most of the time. Whether for productivity or pure laughs, my quality of life is better. Here is a fun suggestion... good to know I'm still needed to write some of the code at least :) #GitHubCopilot #Productivity

...

```
environment_locks: exclusive # pipeline | exclusive - use built in locks or new custom pipeline level locks
environment:
  - name: dev
    skip: false          # skips this environment from automation
    skip_deploy: false   # skips deployment to this environment
    skip_destroy: false  # skips destroy of this environment
    skip_destroy_plan: false # skips destroy plan of this environment
    skip_destroy_apply: false # skips destroy apply of this environment
    skip_destroy_destroy: false # skips destroy destroy of this environment
    skip_destroy_destroy_plan: false # skips destroy destroy plan of this environment
    skip_destroy_destroy_apply: false # skips destroy destroy apply of this environment
    skip_destroy_destroy_destroy: false # skips destroy destroy destroy of this environment
    skip_destroy_destroy_destroy_plan: false # skips destroy destroy destroy plan of this environment
    skip_destroy_destroy_destroy_apply: false # skips destroy destroy destroy apply of this environment
    skip_destroy_destroy_destroy_destroy: false # skips destroy destroy destroy destroy of this environment
    skip_destroy_destroy_destroy_destroy_plan: false # skips destroy destroy destroy destroy plan of this environment
    skip_destroy_destroy_destroy_destroy_apply: false # skips destroy destroy destroy destroy apply of this environment
    skip_destroy_destroy_destroy_destroy_destroy: false # skips destroy destroy destroy destroy destroy of this environment
    skip_destroy_destroy_destroy_destroy_destroy_plan: false # skips destroy destroy destroy destroy destroy plan of this environment
    skip_destroy_destroy_destroy_destroy_destroy_apply: false # skips destroy destroy destroy destroy destroy apply of this environment
    skip_destroy_destroy_destroy_destroy_destroy_destroy: false # skips destroy destroy destroy destroy destroy destroy of this environment
    skip_destroy_destroy_destroy_destroy_destroy_destroy_plan: false # skips destroy destroy destroy destroy destroy destroy plan of this environment
    skip_destroy_destroy_destroy_destroy_destroy_destroy_apply: false # skips destroy destroy destroy destroy destroy destroy apply of this environment
    skip_destroy_destroy_destroy_destroy_destroy_destroy_destroy: false # skips destroy destroy destroy destroy destroy destroy destroy of this environment
```



Frustrating: Hidden Intellisense



Dangerous: Mostly Correct Suggestions



Inconsistent: Style Matching & Linting



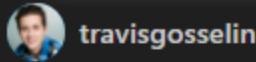
Really?: Prompt / Comment Engineering

# COPilot

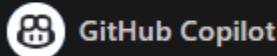
Future with Copilot X

<https://github.com/features/preview/copilot-x>

Chat with GPT-4



Hey copilot - what kinds of things can you help me with?



Sorry, but I can only assist with programming related questions.

Voice

Explanations



### Copilot for CLI

```
+ copilot-cli git:(main) ?? use ffmpeg to add a watermark to input.mp4
----- Command -----
ffmpeg -i input.mp4 -i watermark.png -filter_complex "overlay=10:10" output.mp4
----- Explanation -----
o ffmpeg is used to convert video files.
o -i input.mp4 specifies the input file.
o -i watermark.png specifies the input file.
o -filter_complex "overlay=10:10" specifies the filter to apply.
    o overlay=10:10 specifies that we want to overlay the second input file at position (10, 10).
o output.mp4 specifies the output file.
> Run this command
    • Revise query
    ✘ Cancel
```

Eliminate CLI Docs

Explain What You Want



### Copilot for Pull Requests

Add edges for type assignability #920

Open monalisa wants to merge 2 commits into `main` from `awesome_feature`

monalisa commented 1 second ago · edited by copilot

This pull request adds semantic analysis to the feature extraction plugin, which enhances the feature graph with information about types and assignability of expressions in Java code. It modifies the pom.xml file, the FeaturePlugin.

Code walkthrough

- Import new semantic analysis classes in FeaturePlugin.java ([link](#))
- Create and invoke TypeAnalysis, TypeScanner, and AssignabilityAnalysis on compilation unit in FeaturePlugin.java ([link](#))
- Write type subgraph and add attributes for new edge types in DotOutput.java ([link](#), [link](#))
- Add fields, methods, and constructor logic for type node associations in FeatureGraph.java ([link](#), [link](#), [link](#), [link](#))

generated by copilot

AI-Generated Descriptions

Automating Missed Tests

### Copilot for Docs

How do I vertically center a div?

There are different ways to vertically center a div, depending on the layout and context of your page. One common method is to use flexbox, which is a modern CSS layout module that allows you to align and distribute items in a flexible container. To use flexbox, you need to set the display property of the parent element to flex, and then use the align-items property to center the child element vertically. For example:

```
/* Parent element */
.container {
  display: flex;
  align-items: center;
  height: 300px; /* optional, but you need some height for the centering to work */
}

/* Child element */
.div {
  width: 200px;
  height: 100px;
  background-color: lightblue;
}
```

Popular Public Docs

Internal Docs? GitHub Pages?

# COPilot

"

The skills of the developer will be to figure out, 'How small do I have to go until I can leverage AI to synthesize that code for me?'

Thomas Dohmke, CEO GitHub

"



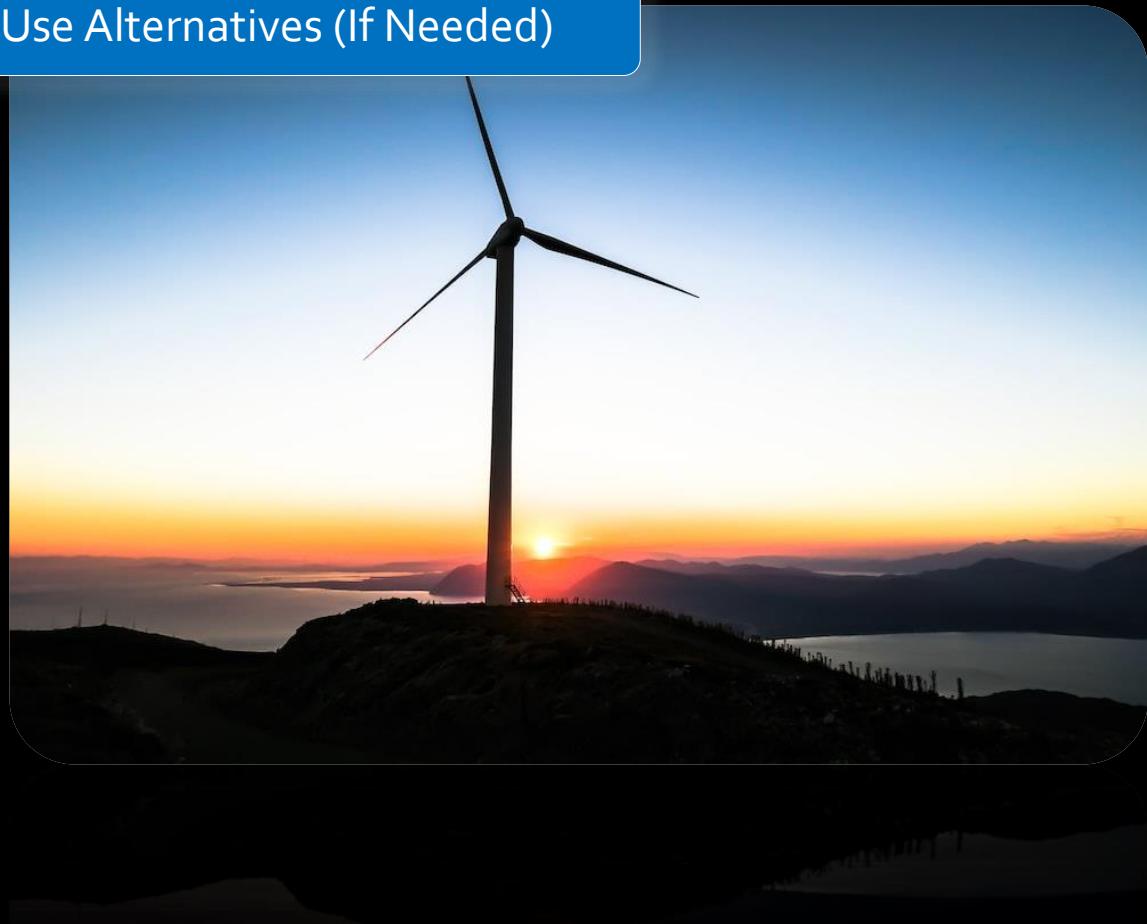
# The GitHub Ecosystem

Mileage Varies Based on Organizational Strengths and Maturity



Measure Your Success

Use Alternatives (If Needed)

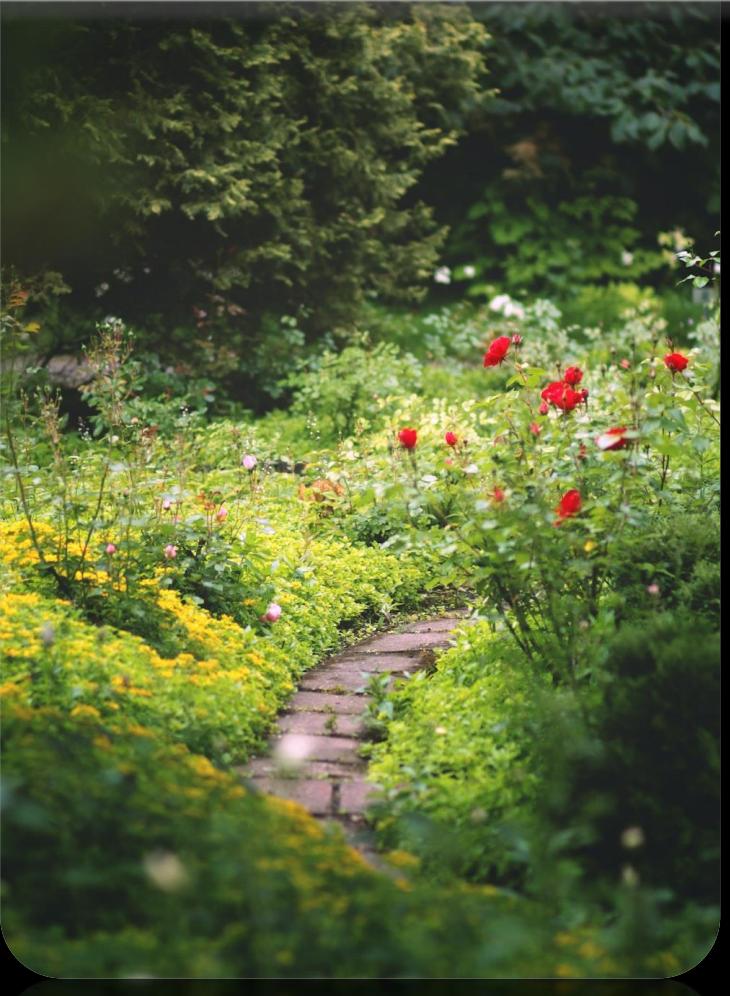


"

Developers work in rainforests, not planned gardens.

"

[a16z.com](http://a16z.com)



## BEYOND SOURCE CONTROL: LEVELING UP WITH THE GITHUB TOOLCHAIN



TRAVIS GOSSELIN 

[travisgosselin.com](http://travisgosselin.com) 

[linkedin.com/in/travisgosselin](https://linkedin.com/in/travisgosselin) 

@travisjgosselin 