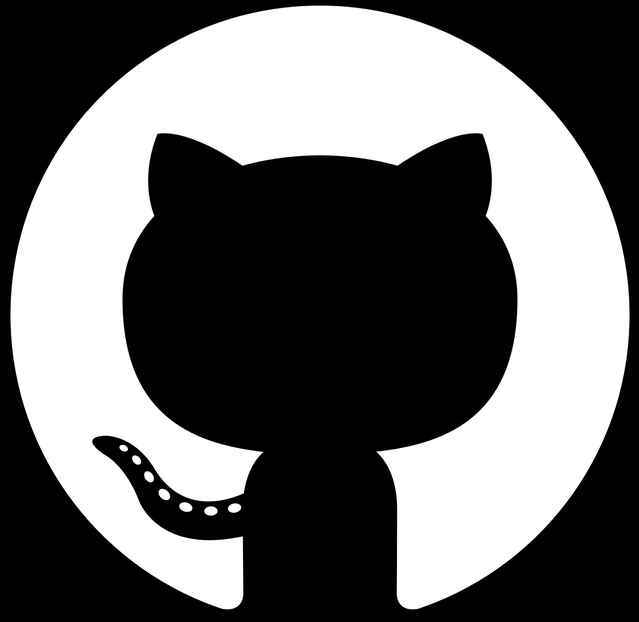


> sessions/featured/

Satellite
VIRTUAL 2020

Securing the software supply chain together

Maya Kaczorowski
Product Manager, GitHub

Agenda

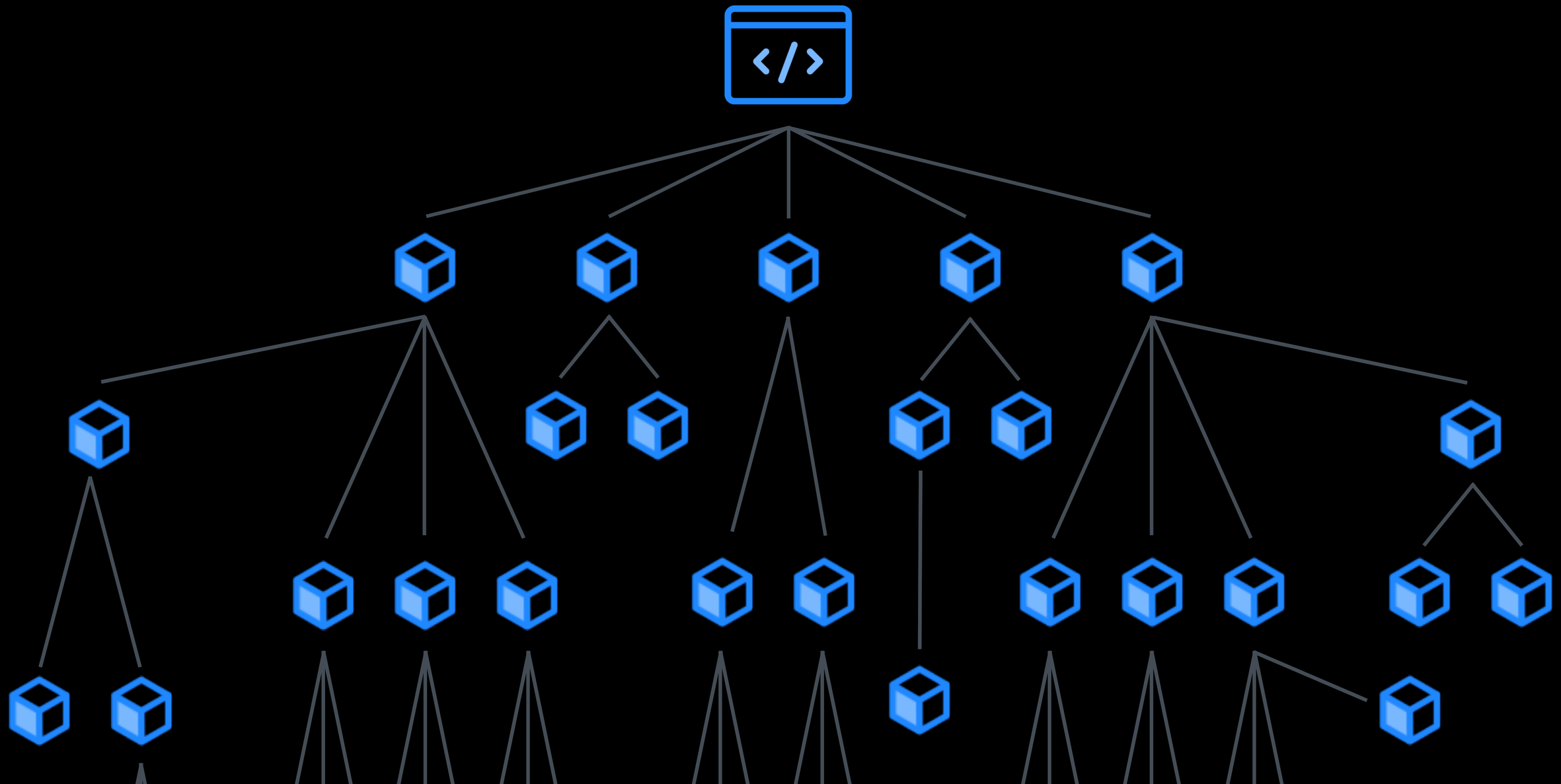
What’s a software supply chain?

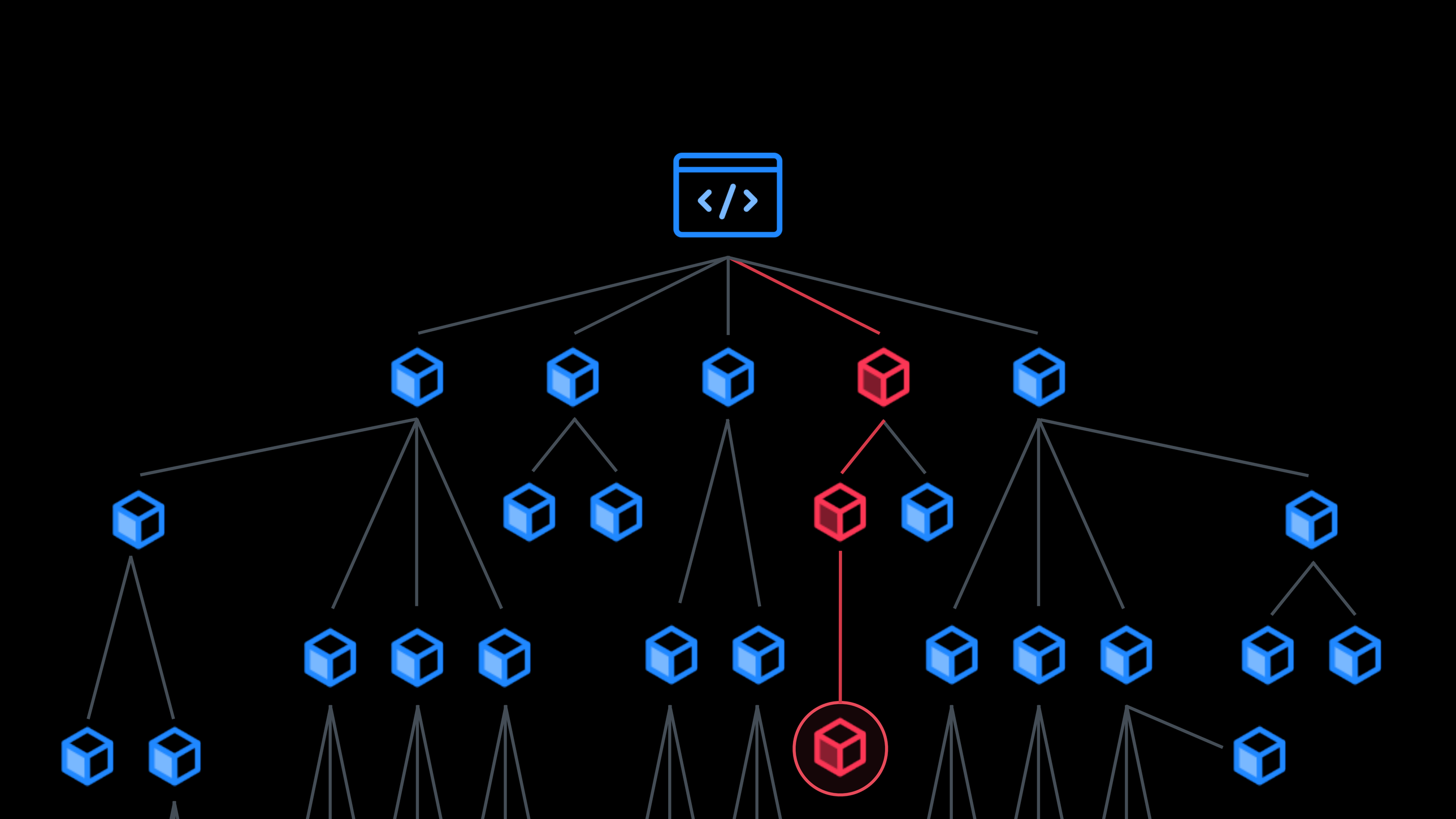
How GitHub helps you

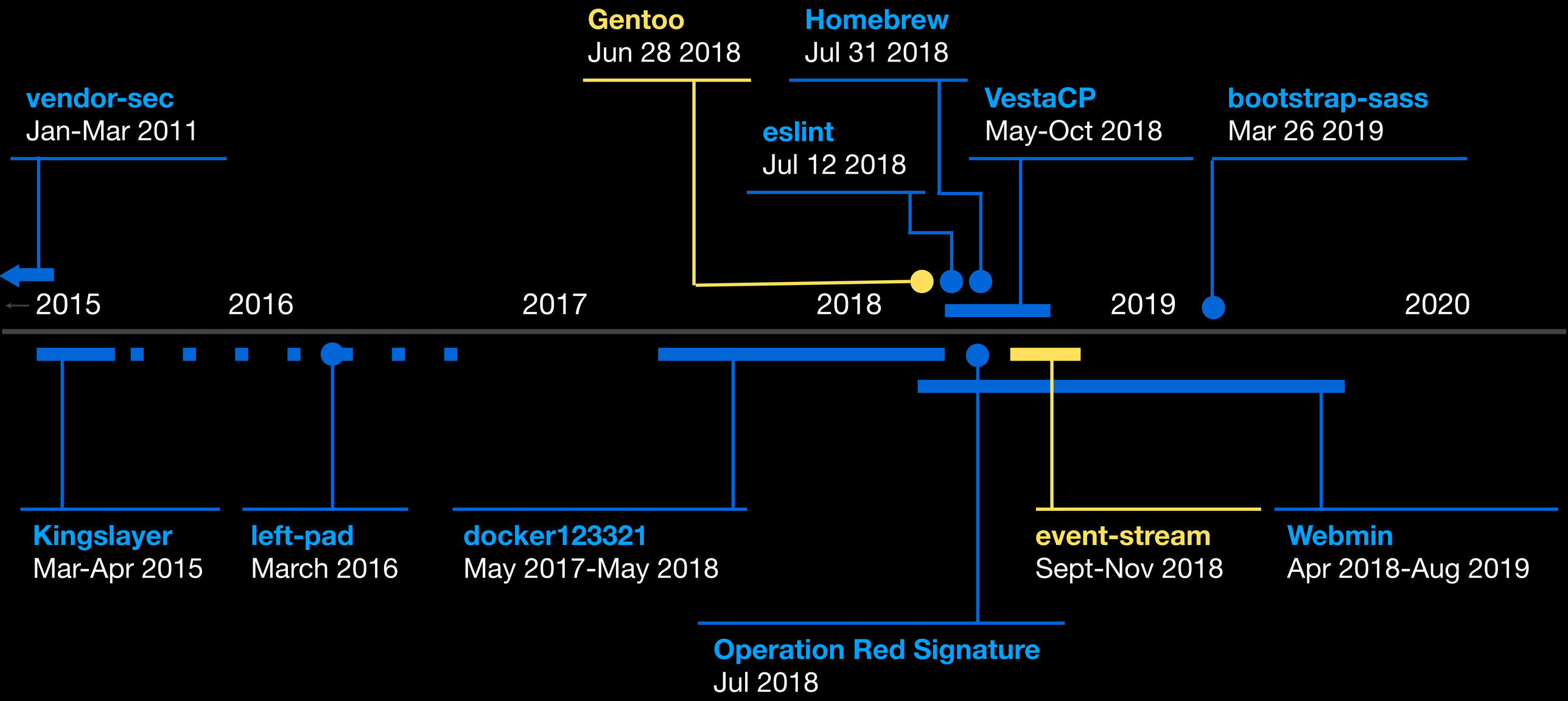
Summary

A software supply chain is anything that touches your code

- from development, through your CI/CD pipeline, until it gets deployed into production.







Timeline of select (known) Software Supply Chain attacks

85% of open source vulnerabilities are disclosed with a **fix already available**

State of Open Source Security Vulnerabilities, 2020, WhiteSource

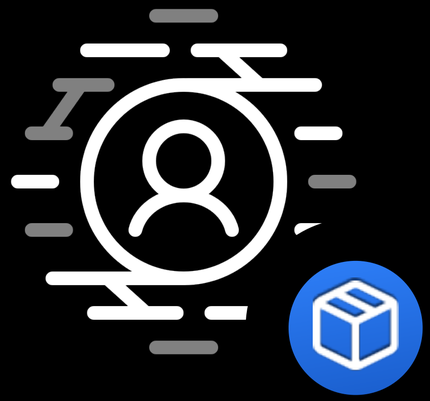
52% of developers find it “painful” to update vulnerable component releases

State of the Software Supply Chain Report, 2019, Sonatype

Ensure the open source community has the **tools** they need

Provide **information** so you can decide how to consume dependencies

Control what code, binaries and packages you use based on your requirements



Developers

Maintainers

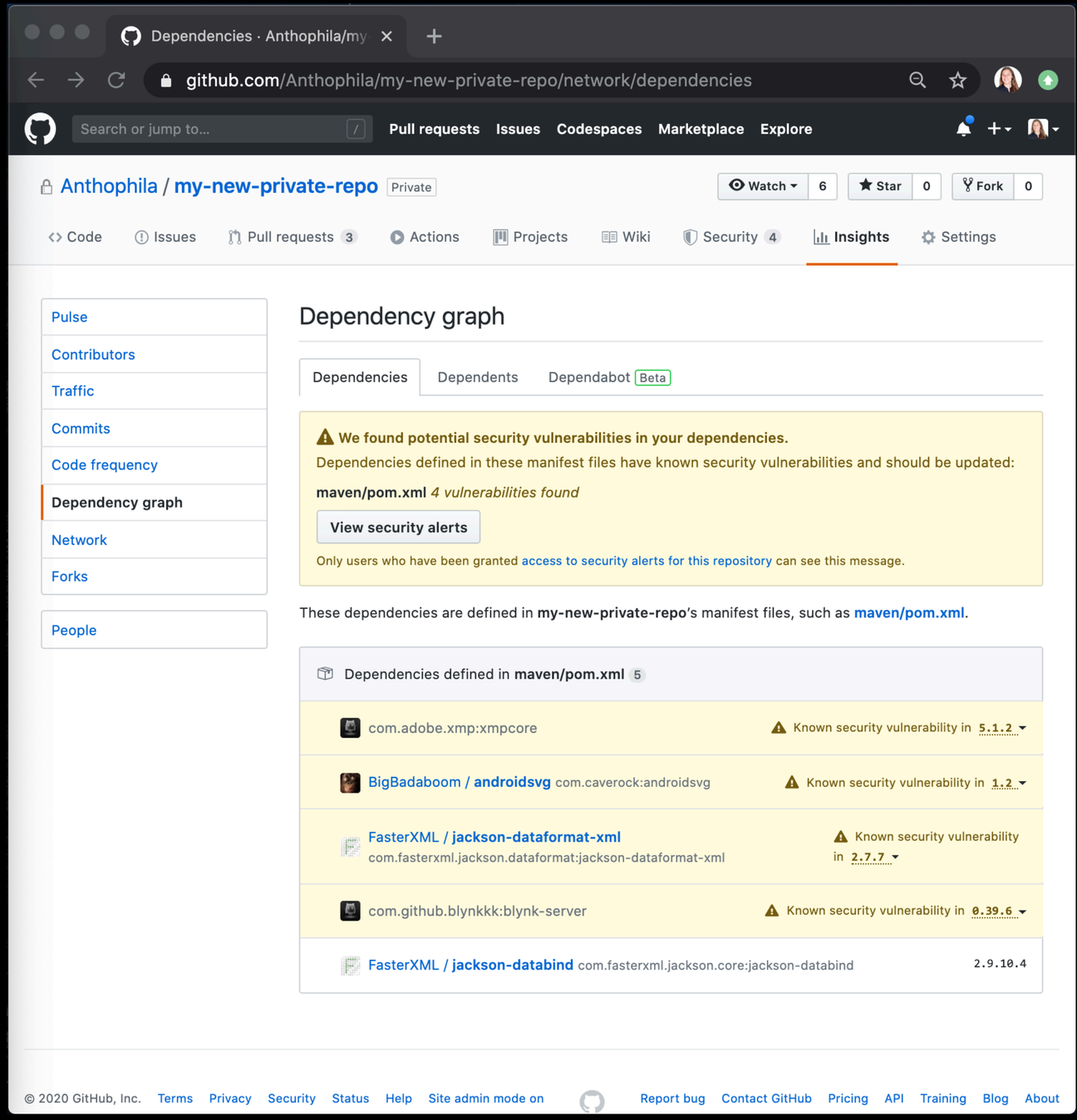
Security Researchers

Dependency Graph

Parses manifest files for dependencies

Items added when a push to the default branch is made

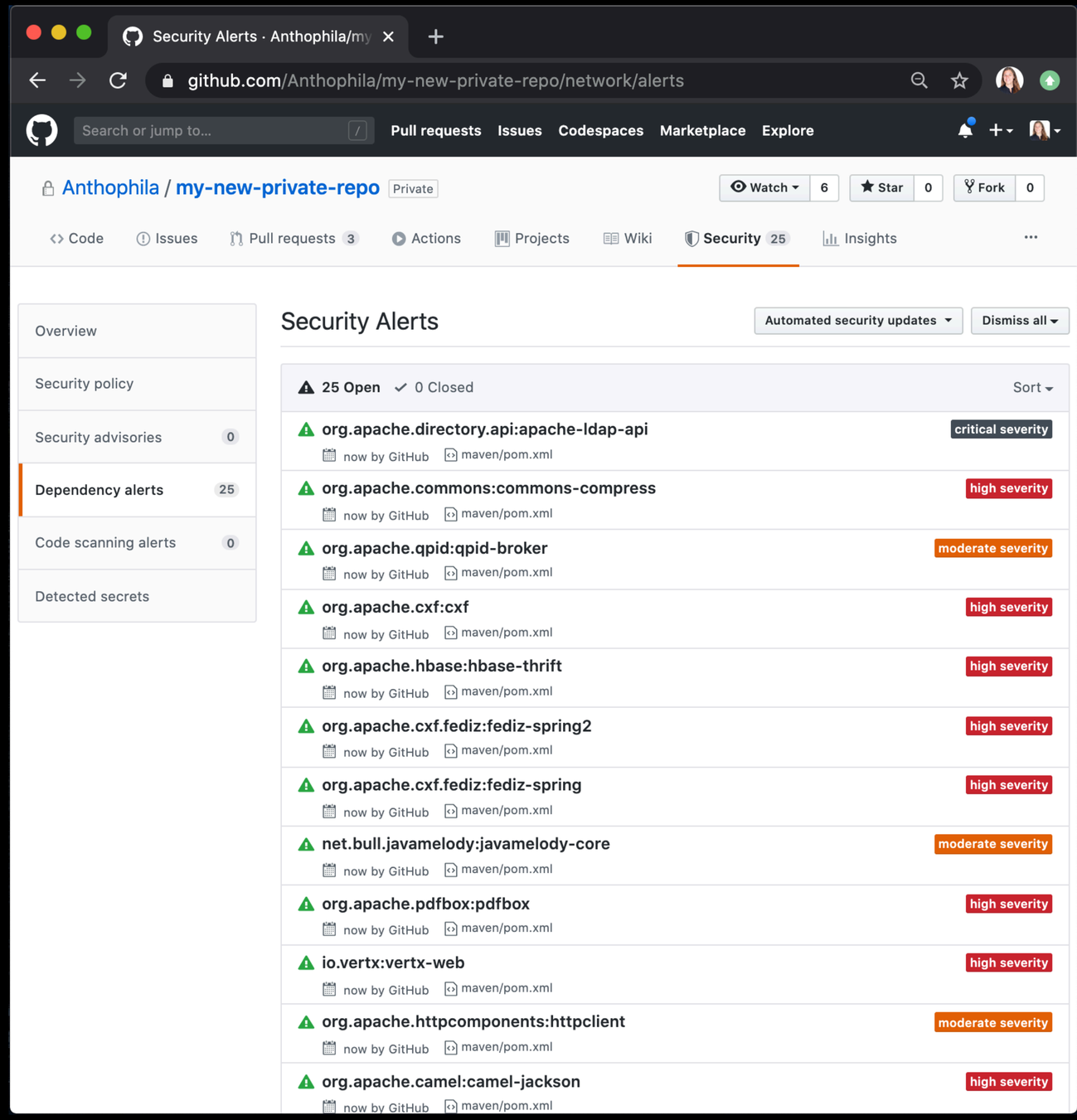
Scans for JavaScript, Java, .NET, PHP, Python and Ruby dependencies



Security alerts for vulnerable dependencies

Notifies you of vulnerabilities in code dependencies

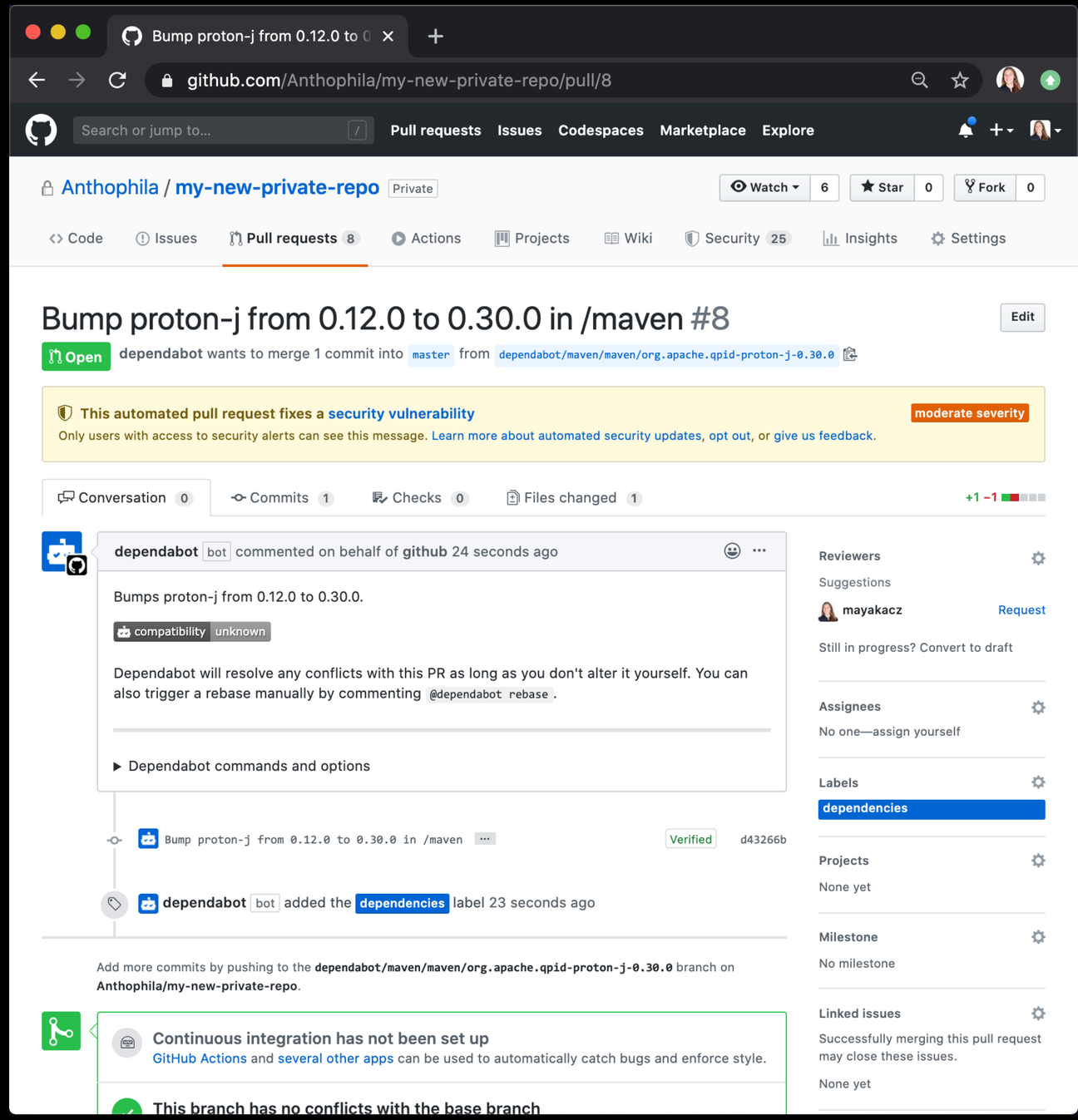
Generated automatically when a new vulnerable dependency is found



Dependabot security updates

Sends you a pull request to move to a fixed version

Generated automatically



>750k

Dependabot PRs merged

40 days

Mean time to remediate (MTTR)
for repos with Dependabot security updates

180+ days

Mean time to remediate (MTTR)
Industry norm

Dependabot version updates

Coming soon

Sends you a pull request to move to a recent version

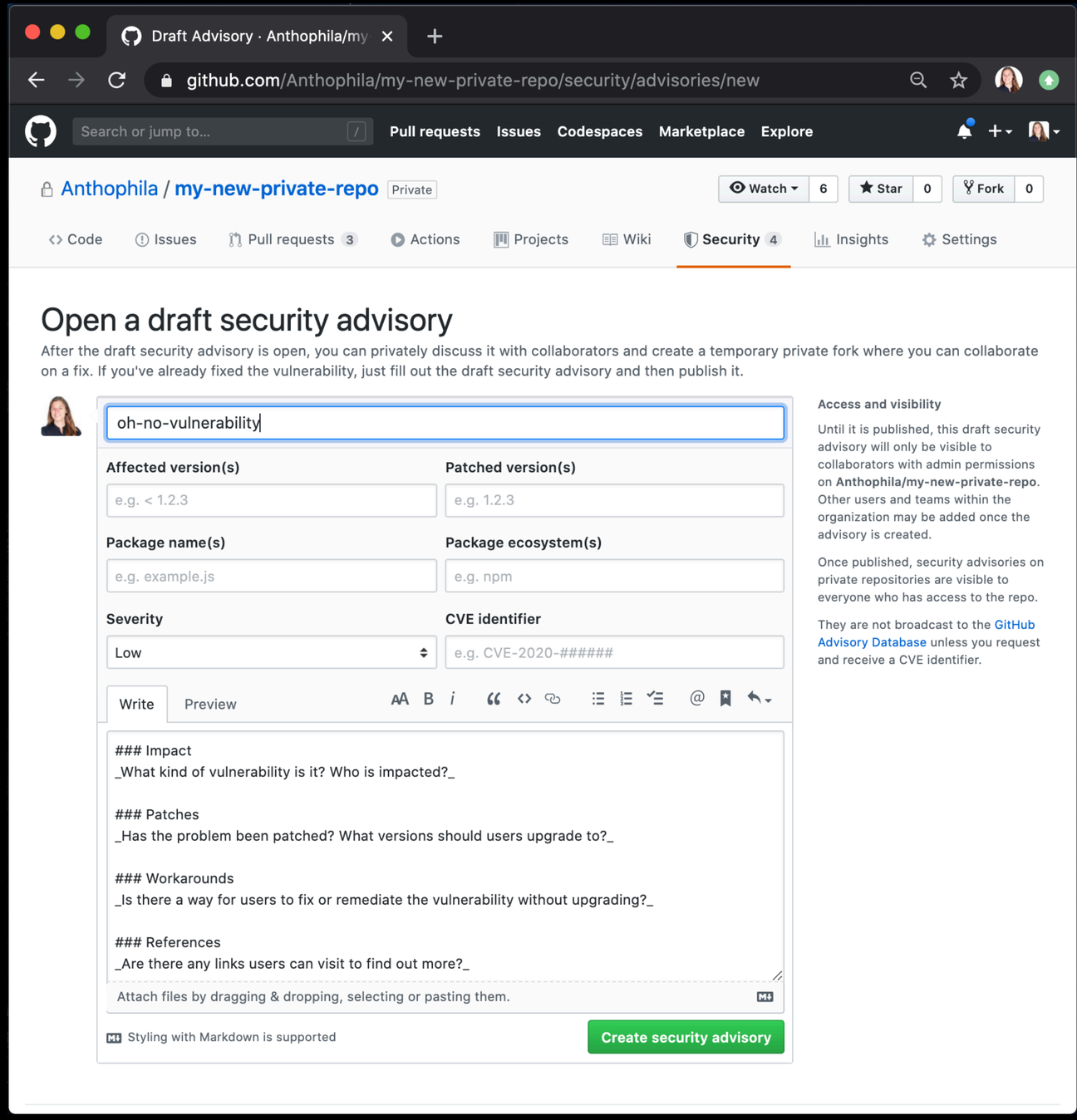
Generated automatically on an ongoing basis

Security Advisories

Disclose a vulnerability in a project hosted on GitHub

If applicable, GitHub can also help you get a CVE

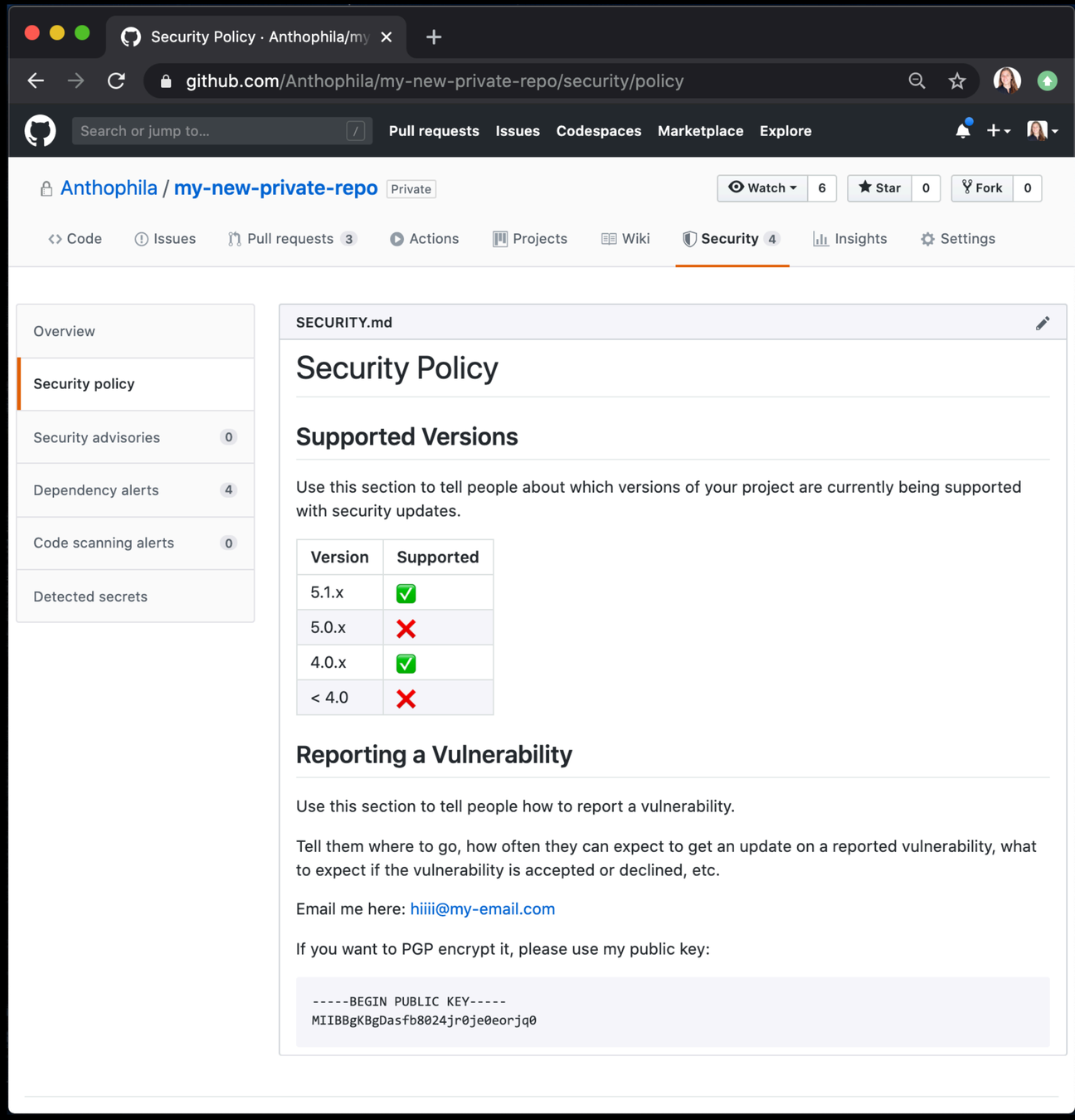
Integrated into GitHub's Advisory Database, which is open source



security.md

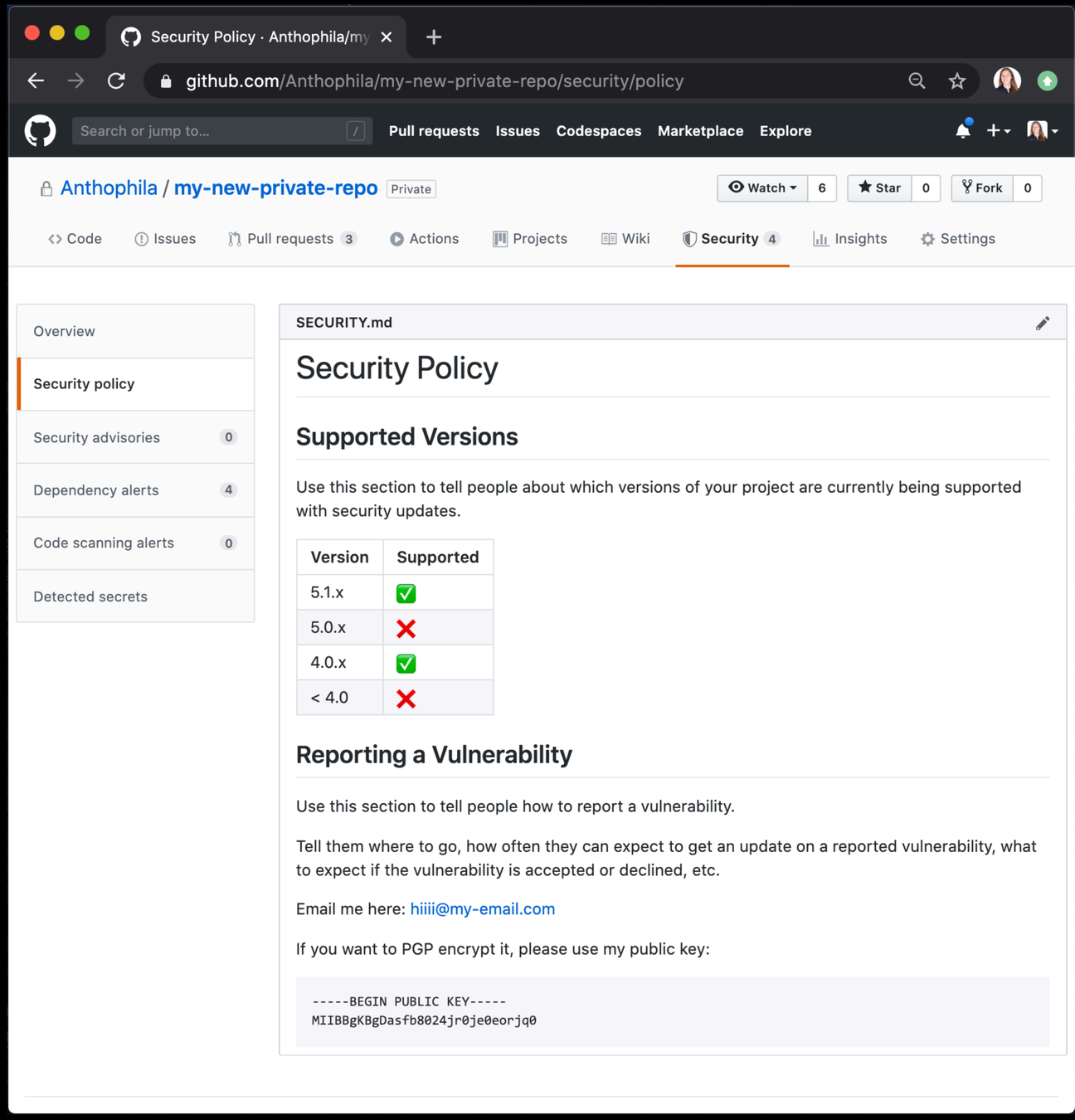
Markdown file in your repo with information on your disclosure and reporting policy

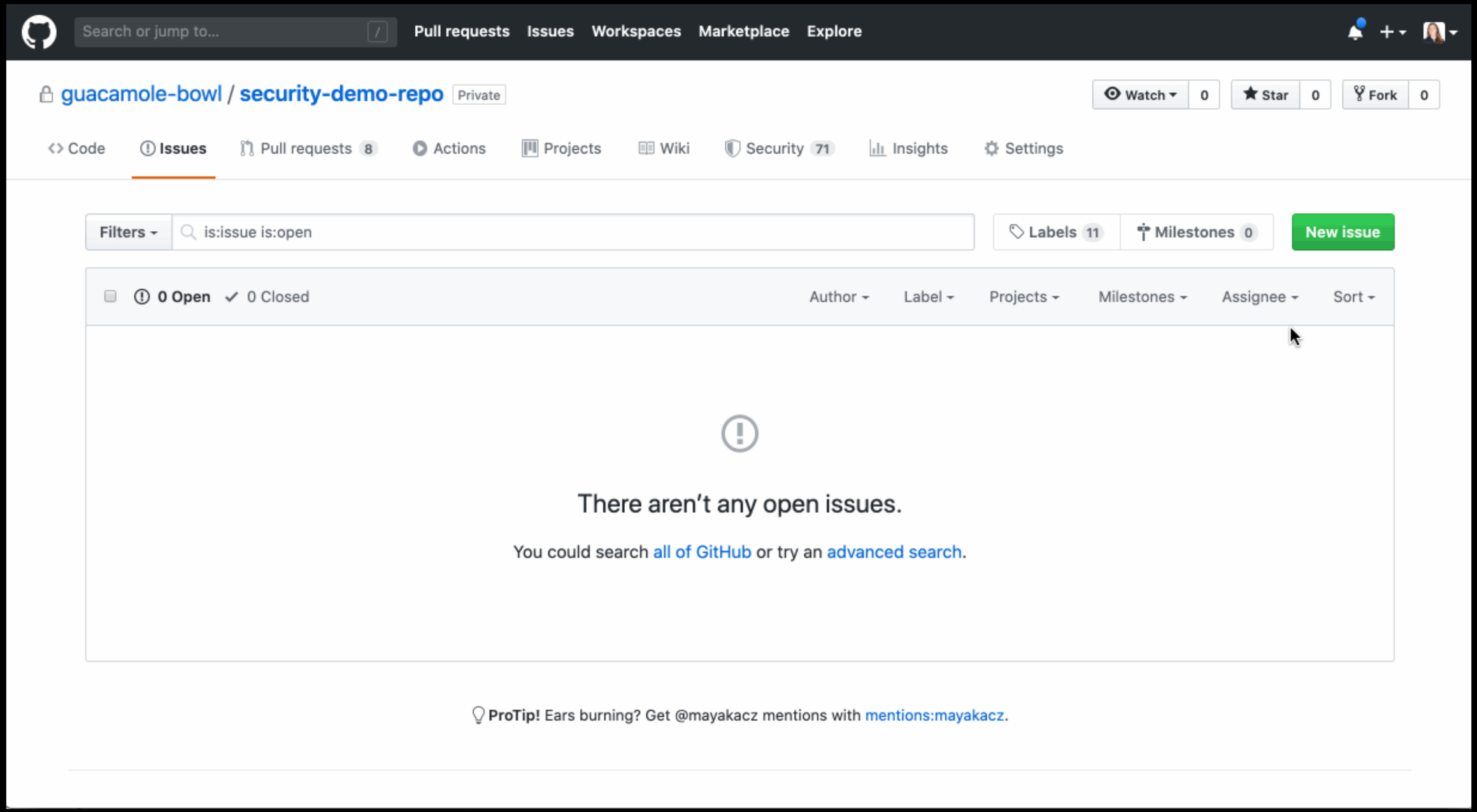
Per-project or apply one across all repos in an organization



security.md

Please report 😊




Search or jump to...
Pull requests
Issues
Workspaces
Marketplace
Explore
guacamole-bowl / security-demo-repo
Private
Watch 0
Star 0
Fork 0
Code
Issues
Pull requests 8
Actions
Projects
Wiki
Security 71
Insights
Settings
Filters
is:issue is:open
Labels 11
Milestones 0
New issue
0 Open
0 Closed
Author
Label
Projects
Milestones
Assignee
Sort
There aren't any open issues.
You could search all of GitHub or try an advanced search.
ProTip! Ears burning? Get @mayakacz mentions with mentions:mayakacz.

Security Advisories - credits

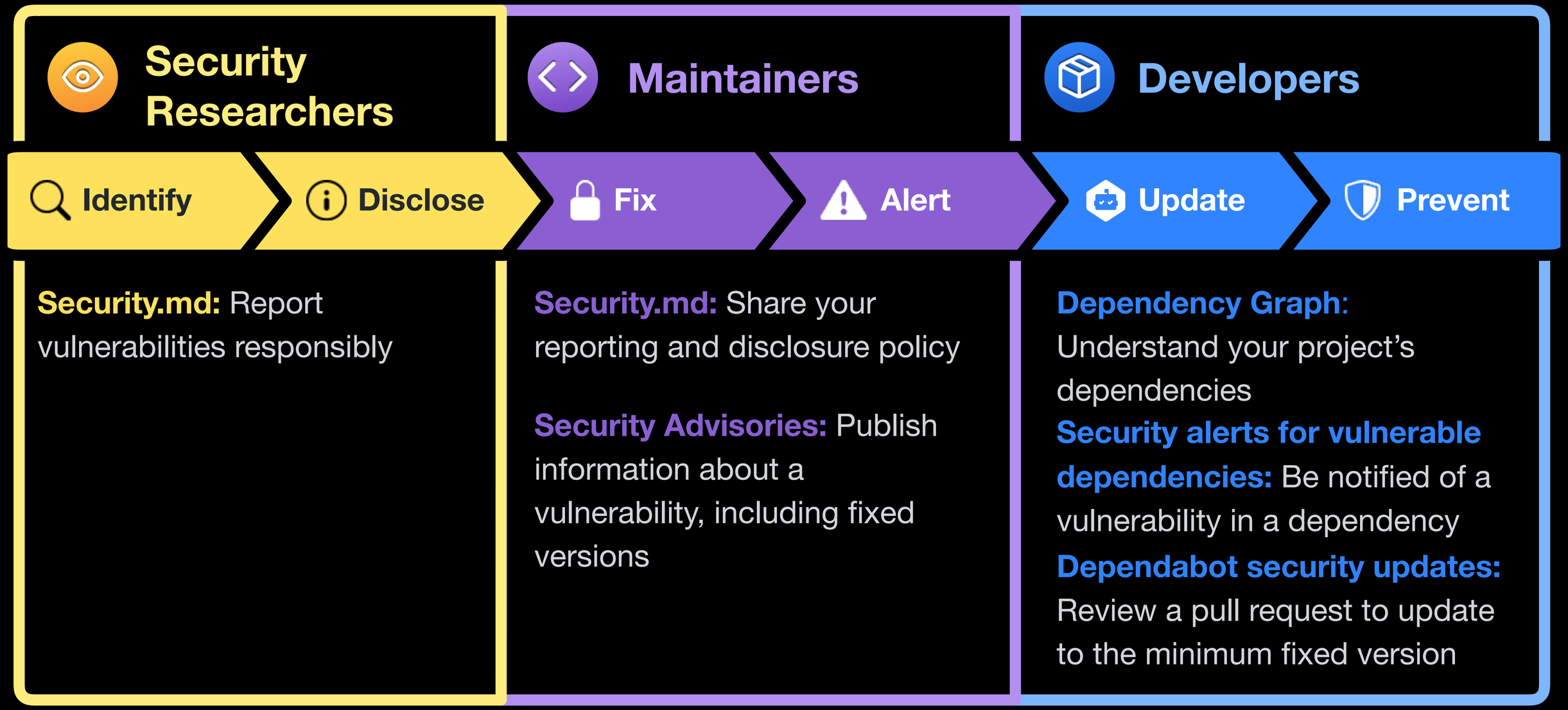
Coming soon

Attribution for helping discover a vulnerability or develop a fix, as part of the advisory

Let’s test it out

- Create a new private repo
- Enable features
- Fix a vulnerable dependency

GitHub helps secure the software supply chain



GitHub secures your complete software life cycle

Supply Chain

Code

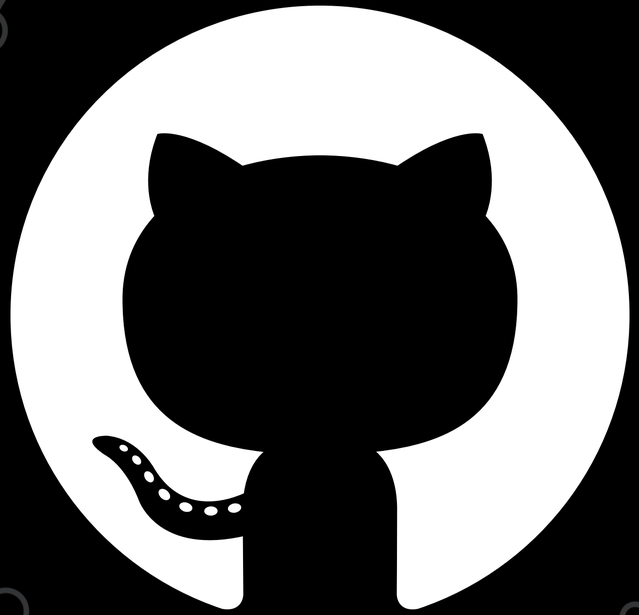
Policies

Platform Security

Learn more

https://github.com/features/security

https://github.co/dependency-graph
https://github.co/security-alerts
https://github.co/security-updates



Q&A