

> sessions/featured/



Securing the software supply chain together

Maya Kaczorowski
Product Manager, GitHub



Agenda

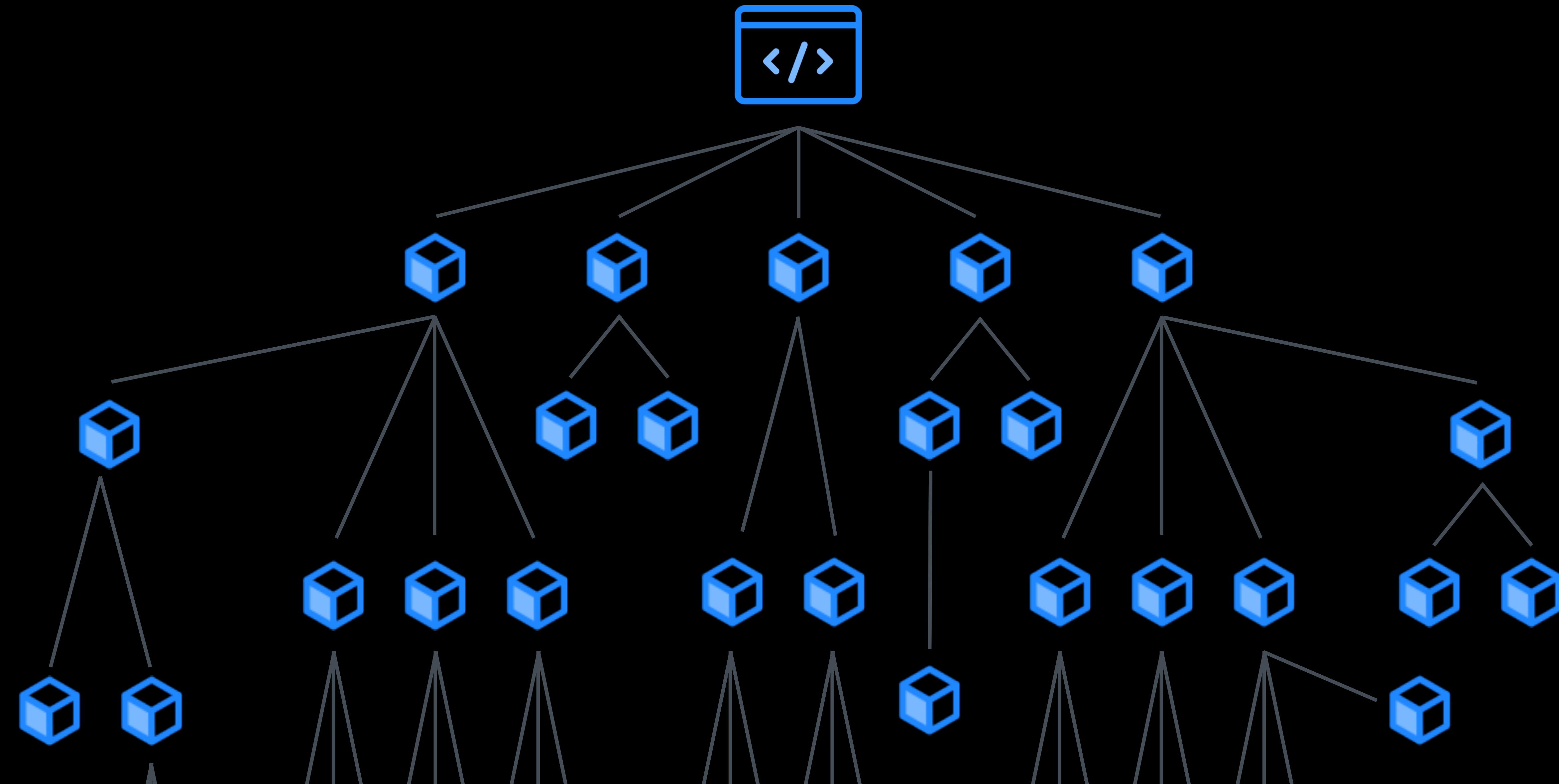
What's a software supply chain?

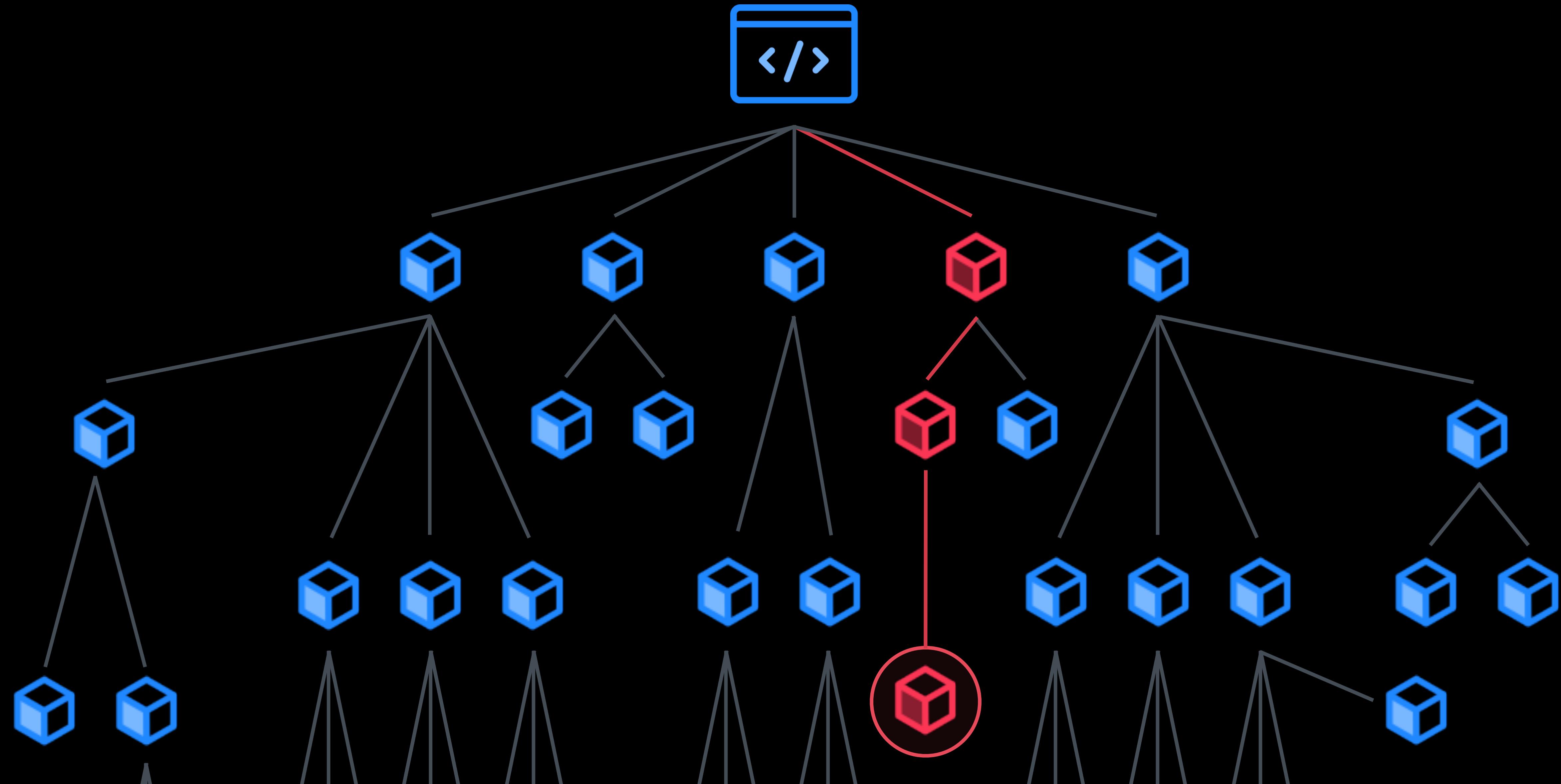
How GitHub helps you

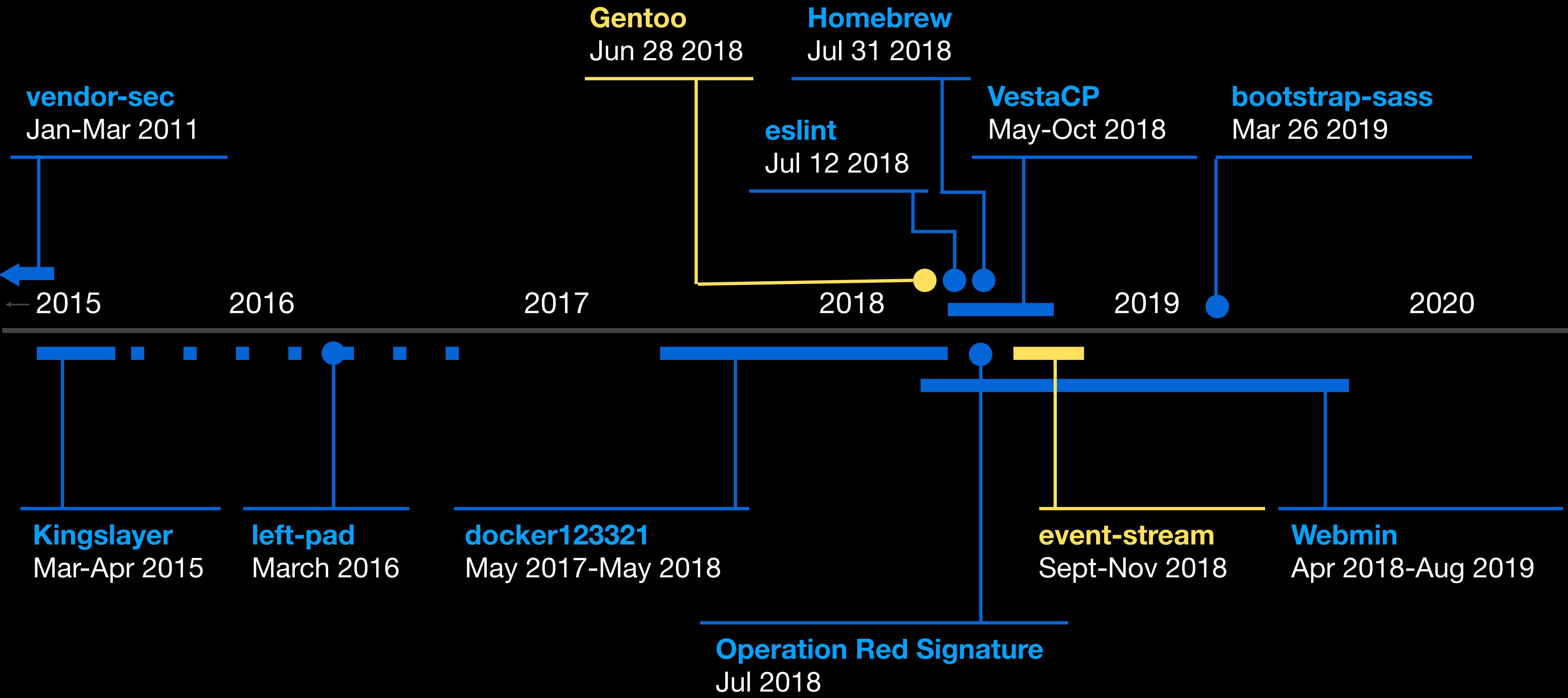
Summary

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**

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



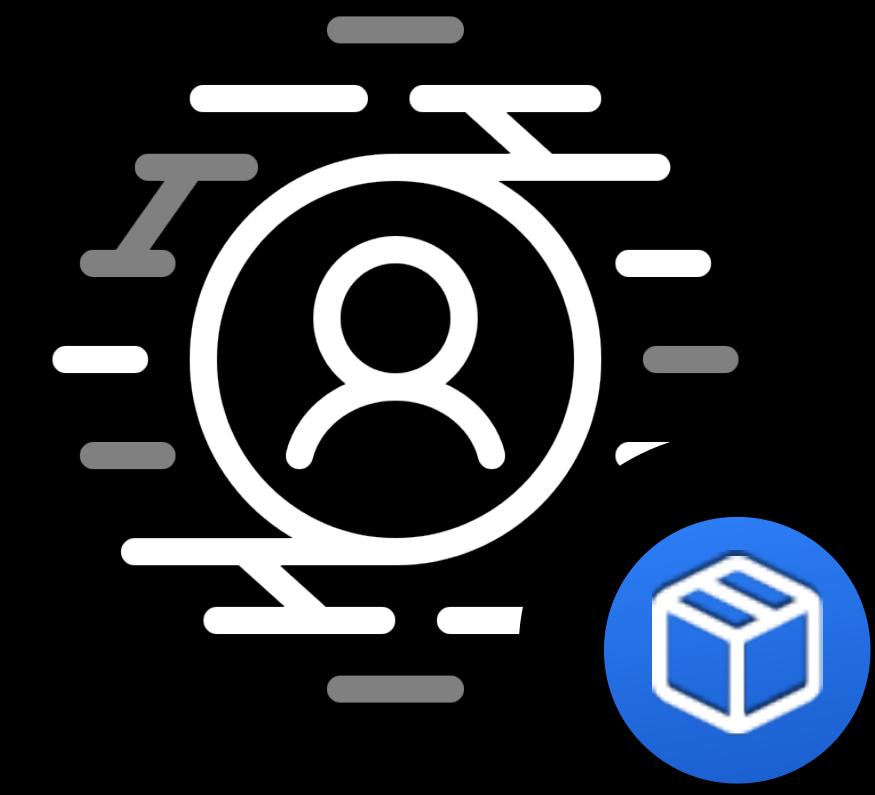
Ensure the open source community has the **tools** they need



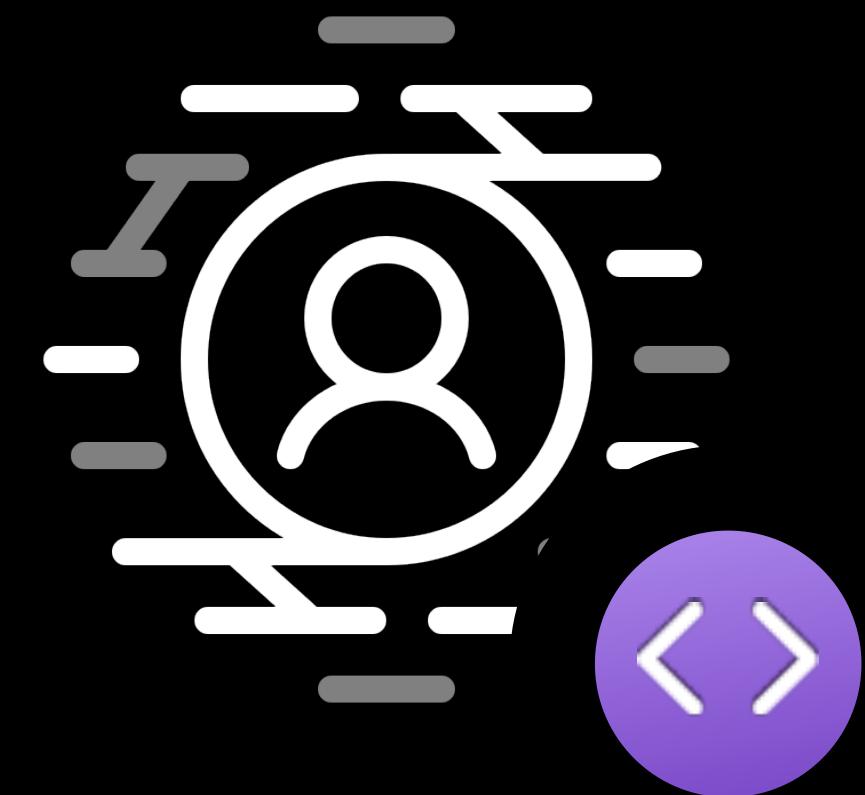
Provide **information** so you can decide how to consume dependencies



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

The screenshot shows a GitHub repository page for 'Anthophila / my-new-private-repo'. The 'Insights' tab is selected. On the left, there's a sidebar with links like Pulse, Contributors, Traffic, Commits, Code frequency, Dependency graph (which is highlighted), Network, Forks, and People. The main area is titled 'Dependency graph' and shows a warning message: '⚠ We found potential security vulnerabilities in your dependencies.' It lists 'Dependencies defined in these manifest files have known security vulnerabilities and should be updated: maven/pom.xml 4 vulnerabilities found'. A 'View security alerts' button is present. Below this, it says 'Only users who have been granted access to security alerts for this repository can see this message.' At the bottom, it lists 'Dependencies defined in maven/pom.xml 5':

Dependency	Vulnerability Details
com.adobe.xmp:xmpcore	⚠ Known security vulnerability in 5.1.2
BigBadaboom / androidsvg com.caverock:androidsvg	⚠ Known security vulnerability in 1.2
FasterXML / jackson-dataformat-xml com.fasterxml.jackson.dataformat:jackson-dataformat-xml	⚠ Known security vulnerability in 2.7.7
com.github.blynkkk:blynk-server	⚠ Known security vulnerability in 0.39.6
FasterXML / jackson-databind com.fasterxml.jackson.core:jackson-databind	2.9.10.4

Security alerts for vulnerable dependencies

Notifies you of vulnerabilities in code dependencies

Generated automatically when a new vulnerable dependency is found

The screenshot shows a GitHub repository named "Anthophila / my-new-private-repo". The "Security" tab is selected, displaying 25 open security alerts. The alerts are listed in descending order of severity, with the first few being critical. Each alert entry includes the dependency name, a link to the GitHub commit, and a link to the Maven/POM XML file.

Dependency	Severity
org.apache.directory.api:apache-ldap-api	Critical
org.apache.commons:commons-compress	High
org.apache.qpid:qpid-broker	Moderate
org.apache.cxf:cxf	High
org.apache.hbase:hbase-thrift	High
org.apache.cxf.fediz:fediz-spring2	High
org.apache.cxf.fediz:fediz-spring	High
net.bull.javamelody:javamelody-core	Moderate
org.apache.pdfbox:pdfbox	High
io.vertx:vertx-web	High
org.apache.httpcomponents:httpclient	Moderate
org.apache.camel:camel-jackson	High

Dependabot security updates

Sends you a pull request
to move to a fixed
version

Generated automatically

The screenshot shows a GitHub pull request page for a repository named "Anthophila / my-new-private-repo". The pull request is titled "Bump proton-j from 0.12.0 to 0.30.0 in /maven #8". The status of the pull request is "Open", and it is merging 1 commit from the "dependabot/maven/maven/org.apache.qpid-proton-j-0.30.0" branch into the "master" branch. A yellow banner at the top indicates that this is an automated pull request fixing a security vulnerability, labeled as "moderate severity". The pull request has 0 conversations, 1 commit, 0 checks, and 1 file changed. The commit message is "Bumps proton-j from 0.12.0 to 0.30.0." and includes a note about compatibility being unknown. The commit is verified and has a SHA of d43266b. The Dependabot bot added the "dependencies" label 23 seconds ago. A note at the bottom of the commit says to add more commits by pushing to the "dependabot/maven/maven/org.apache.qpid-proton-j-0.30.0" branch. A green box at the bottom left indicates that continuous integration has not been set up, and another green box at the bottom right indicates that the branch has no conflicts with the base branch. The right sidebar shows repository details like 6 stars, 0 forks, and 25 security issues.

>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

The screenshot shows a GitHub repository named "Anthophila / my-new-private-repo" with a draft security advisory titled "oh-no-vulnerability". The interface includes fields for affected and patched versions, package names and ecosystems, severity, and a CVE identifier. It also features sections for Impact, Patches, Workarounds, and References, along with a rich text editor toolbar. A sidebar provides information about access and visibility, stating that until published, the advisory is visible only to collaborators with admin permissions. It also notes that once published, it becomes visible to everyone with access to the repo and is not broadcast to the GitHub Advisory Database unless requested.

Draft Advisory · Anthophila/my-new-private-repo

github.com/Anthophila/my-new-private-repo/security/advisories/new

Anthophila / my-new-private-repo Private

Code Issues Pull requests 3 Actions Projects Wiki Security 4 Insights Settings

oh-no-vulnerability

Affected version(s) e.g. < 1.2.3 Patched version(s) e.g. 1.2.3

Package name(s) e.g. example.js Package ecosystem(s) e.g. npm

Severity Low CVE identifier e.g. CVE-2020-#####

Write Preview

Access and visibility

Until it is published, this draft security advisory will only be visible to collaborators with admin permissions on Anthophila/my-new-private-repo. Other users and teams within the organization may be added once the advisory is created.

Once published, security advisories on private repositories are visible to everyone who has access to the repo.

They are not broadcast to the GitHub Advisory Database unless you request and receive a CVE identifier.

Impact
What kind of vulnerability is it? Who is impacted?

Patches
Has the problem been patched? What versions should users upgrade to?

Workarounds
Is there a way for users to fix or remediate the vulnerability without upgrading?

References
Are there any links users can visit to find out more?

Attach files by dragging & dropping, selecting or pasting them.

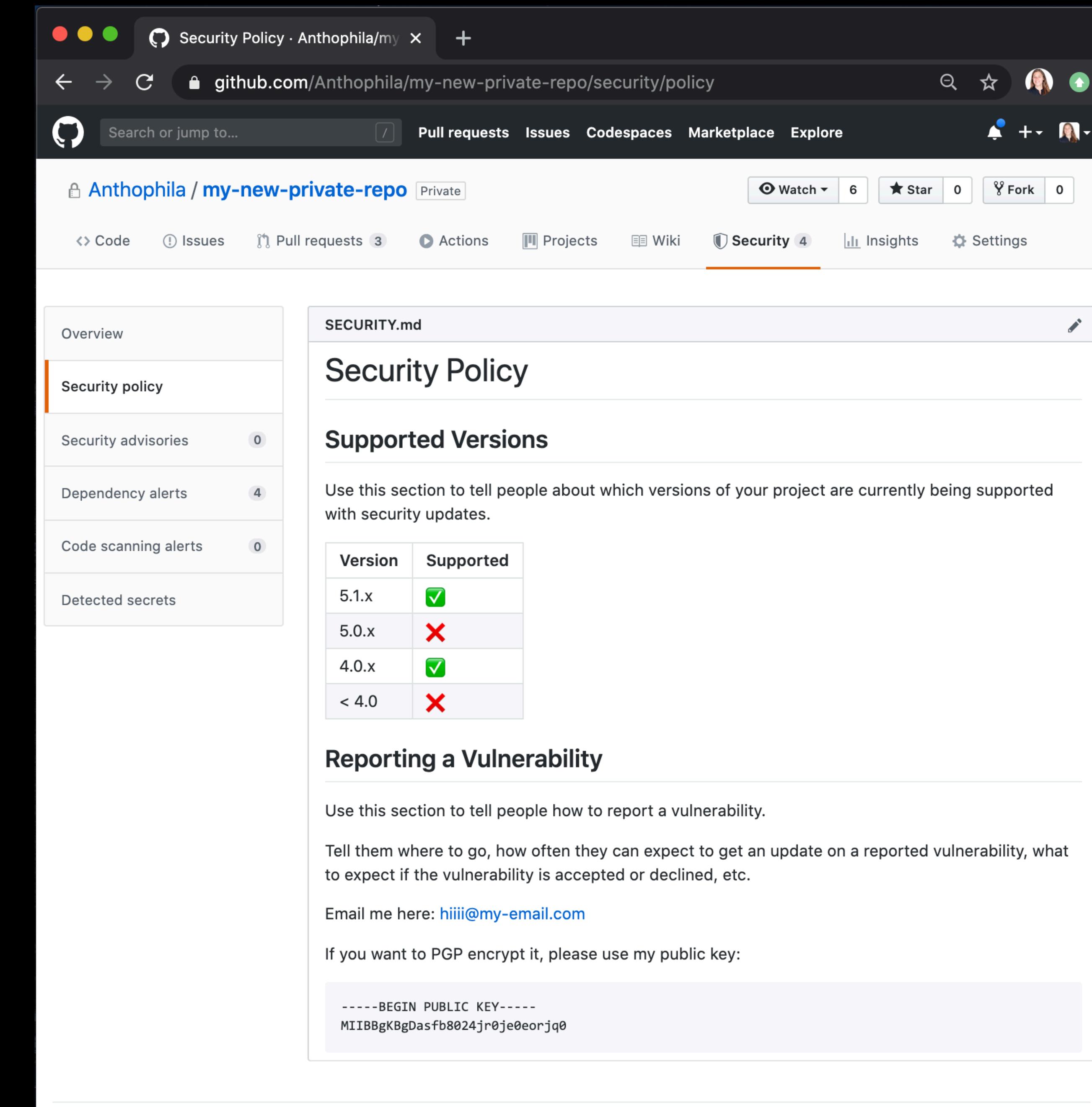
Styling with Markdown is supported

Create security advisory

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



The screenshot shows a GitHub repository named "Anthophila / my-new-private-repo". The "Security" tab is selected, indicated by an orange underline. On the left, there's a sidebar with links: Overview, Security policy (which is active), Security advisories (0), Dependency alerts (4), Code scanning alerts (0), and Detected secrets. The main content area is titled "SECURITY.md" and contains the following sections:

- Security Policy**
- Supported Versions**

Use this section to tell people about which versions of your project are currently being supported with security updates.

Version	Supported
5.1.x	✓
5.0.x	✗
4.0.x	✓
< 4.0	✗
- Reporting a Vulnerability**

Use this section to tell people how to report a vulnerability. Tell them where to go, how often they can expect to get an update on a reported vulnerability, what to expect if the vulnerability is accepted or declined, etc.

Email me here: hiiii@my-email.com

If you want to PGP encrypt it, please use my public key:

```
-----BEGIN PUBLIC KEY-----  
MIIBBgKBgDasfb8024jr0je0eorjq0
```

security.md

Please report 😊

The screenshot shows a GitHub repository named 'Anthophila / my-new-private-repo'. The 'Security' tab is selected in the navigation bar. On the left, a sidebar lists 'Overview', 'Security policy' (which is active), 'Security advisories 0', 'Dependency alerts 4', 'Code scanning alerts 0', and 'Detected secrets'. The main content area is titled 'SECURITY.md' and contains a section for 'Supported Versions' with a table, 'Reporting a Vulnerability' with instructions and an email address, and a public PGP key.

SECURITY.md

Security Policy

Supported Versions

Use this section to tell people about which versions of your project are currently being supported with security updates.

Version	Supported
5.1.x	✓
5.0.x	✗
4.0.x	✓
< 4.0	✗

Reporting a Vulnerability

Use this section to tell people how to report a vulnerability.

Tell them where to go, how often they can expect to get an update on a reported vulnerability, what to expect if the vulnerability is accepted or declined, etc.

Email me here: hiiii@my-email.com

If you want to PGP encrypt it, please use my public key:

```
-----BEGIN PUBLIC KEY-----  
MIIBBgKBgDasfb8024jr0je0eorjq0
```



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

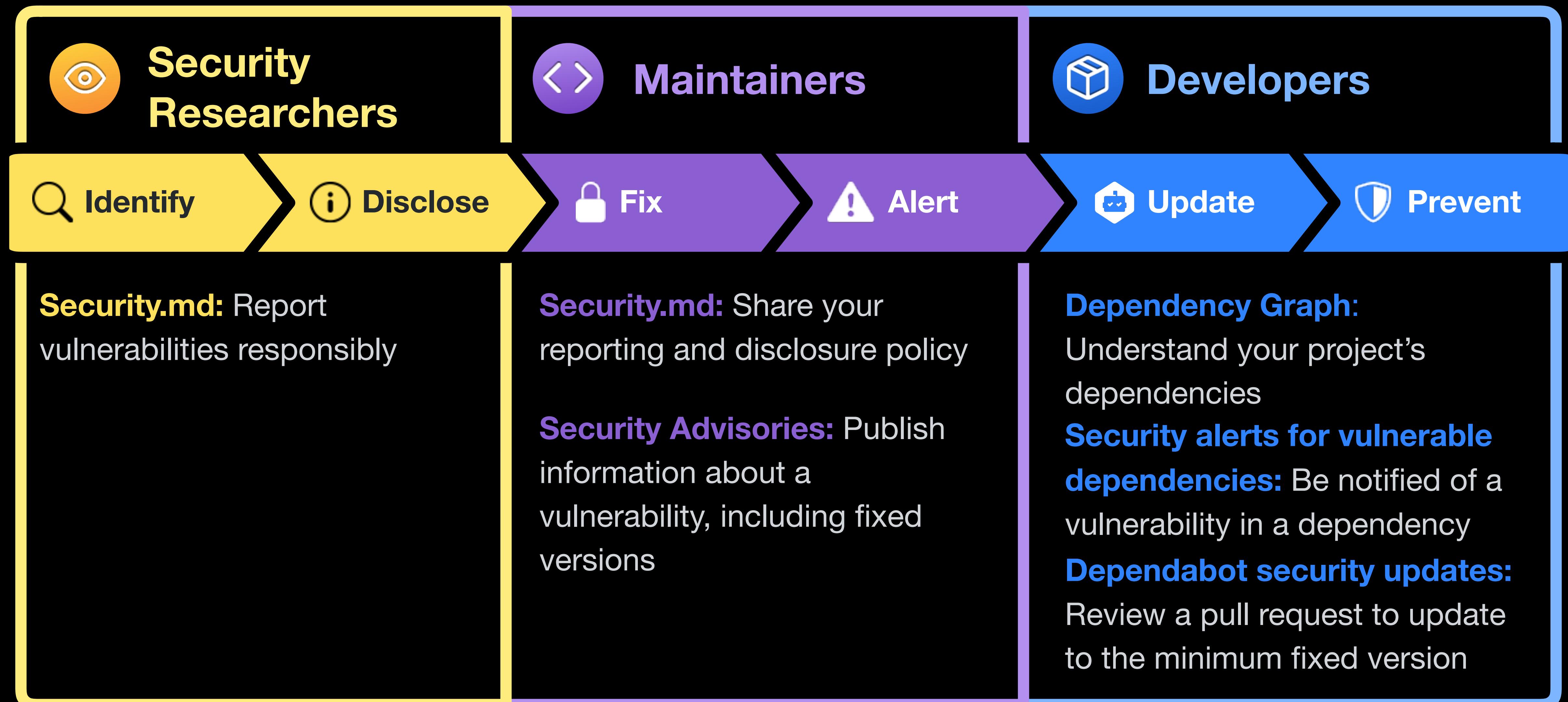


Let's test it out



- 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

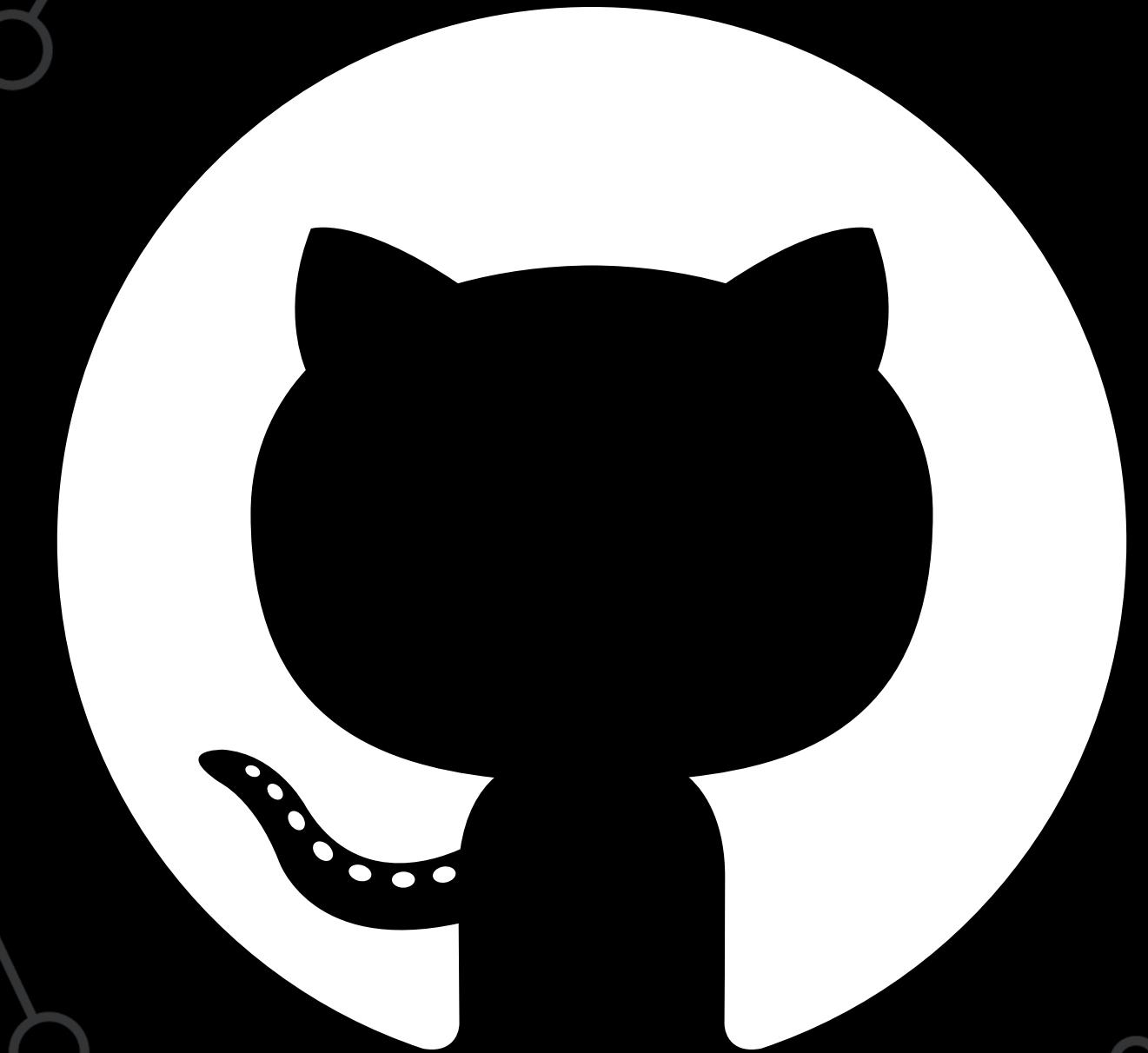
Learn more

<https://github.com/features/security>

<https://github.co/dependency-graph>

<https://github.co/security-alerts>

<https://github.co/security-updates>



Q&A