100M+ Developers, Security, and AI

My journey from DevOps to an AI-assisted future

@jacobdepriest

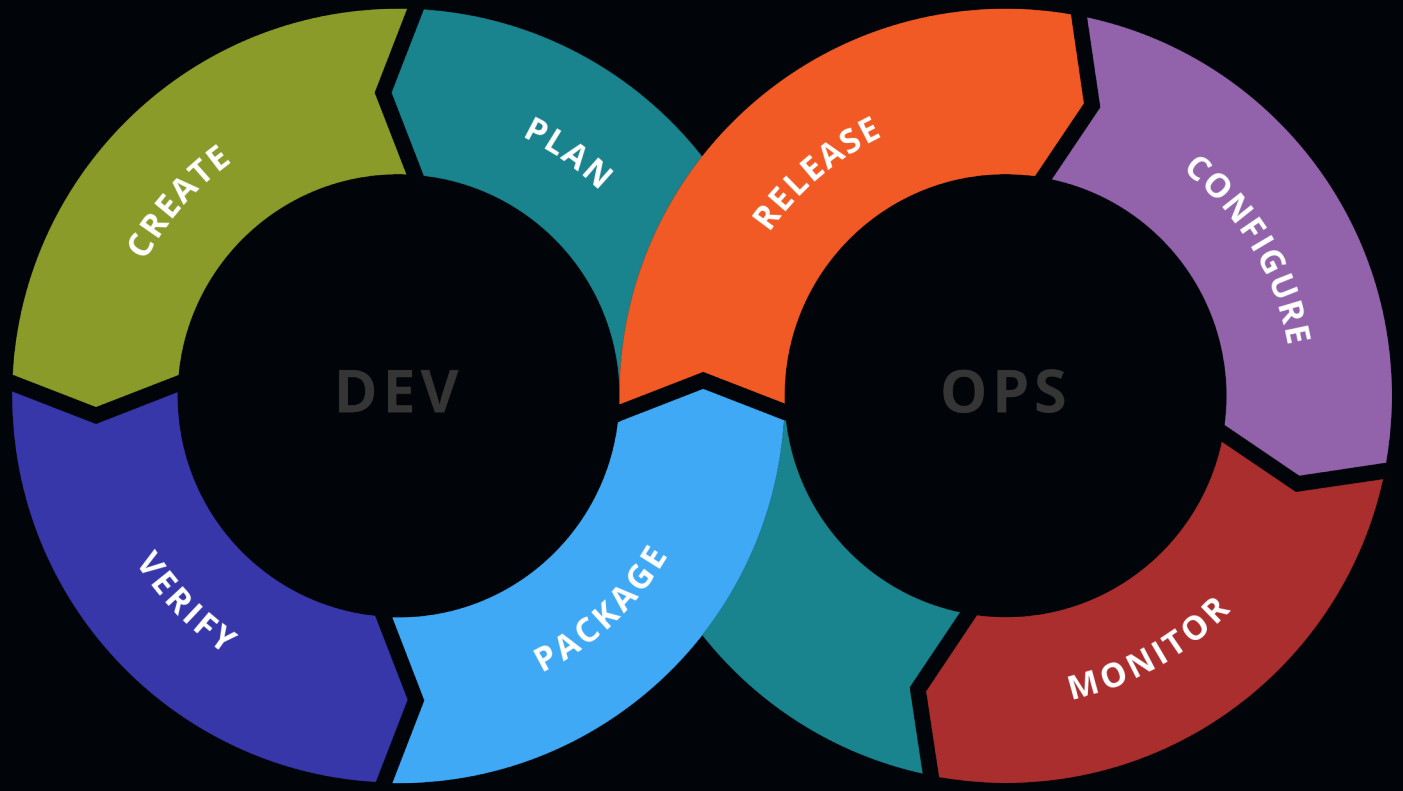
Jacob DePriest

VP, Deputy CSO

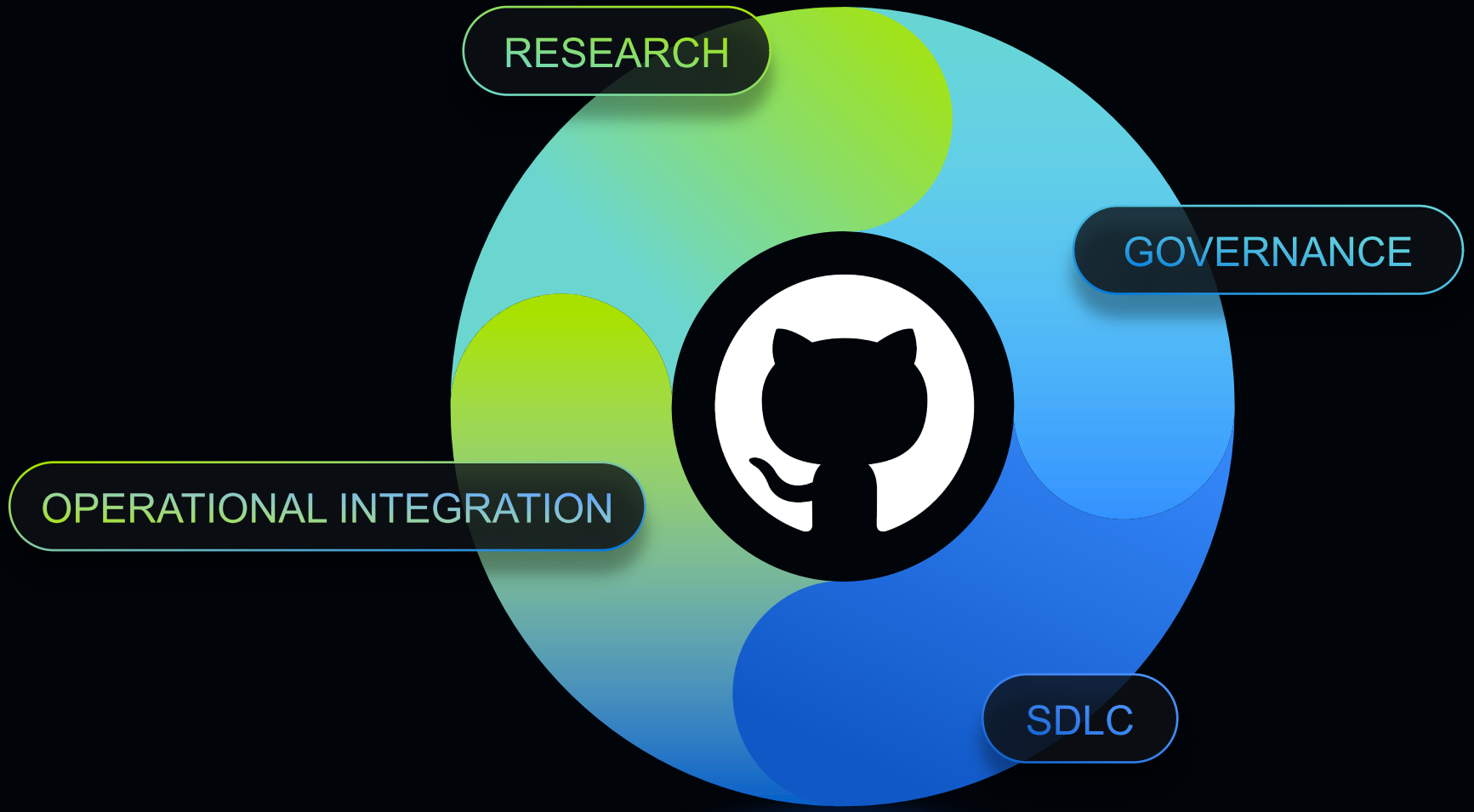
How’d we get here?

Open Source Software

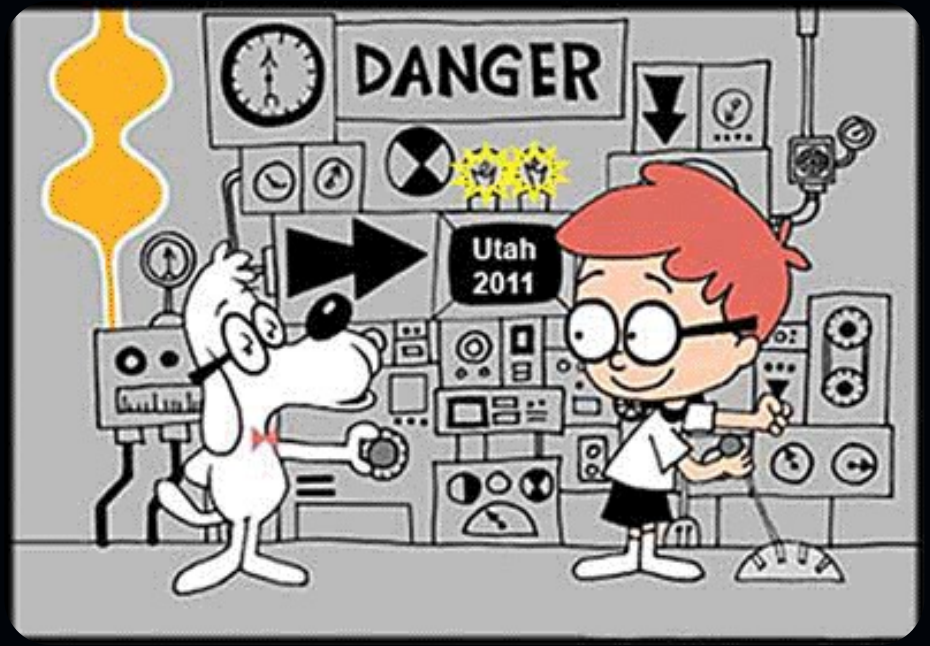
DevX


CREATE
PLAN
RELEASE
CONFIGURE
DEV
OPS
VERIFY
PACKAGE
MONITOR

Unclass Work & Cyber Collaboration


RESEARCH
GOVERNANCE
OPERATIONAL INTEGRATION
SDLC

DevSecOps
at GitHub



GitHub

Then & now

2011 - 2012

2M

Repositories

WORKING ASYNCHRONOUSLY:

Optimize for developer Happiness

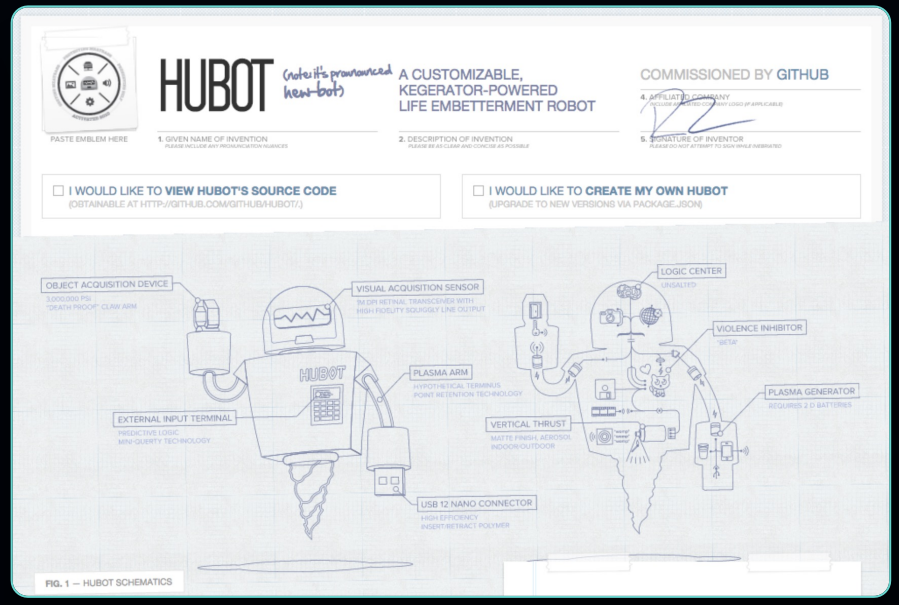
NO MEETINGS • NO DEADLINES • NO MANAGERS

pull requests + branching

2014 - 2018

21M

Repositories

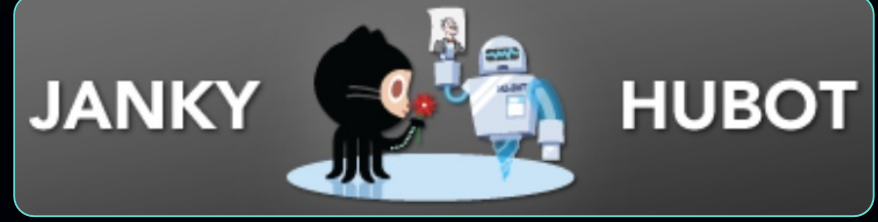


Asynchronous

Focus workflow on code, not meetings

A typical deployment flow

Development → Staging → Production



2018 - 2022

100M

Repositories

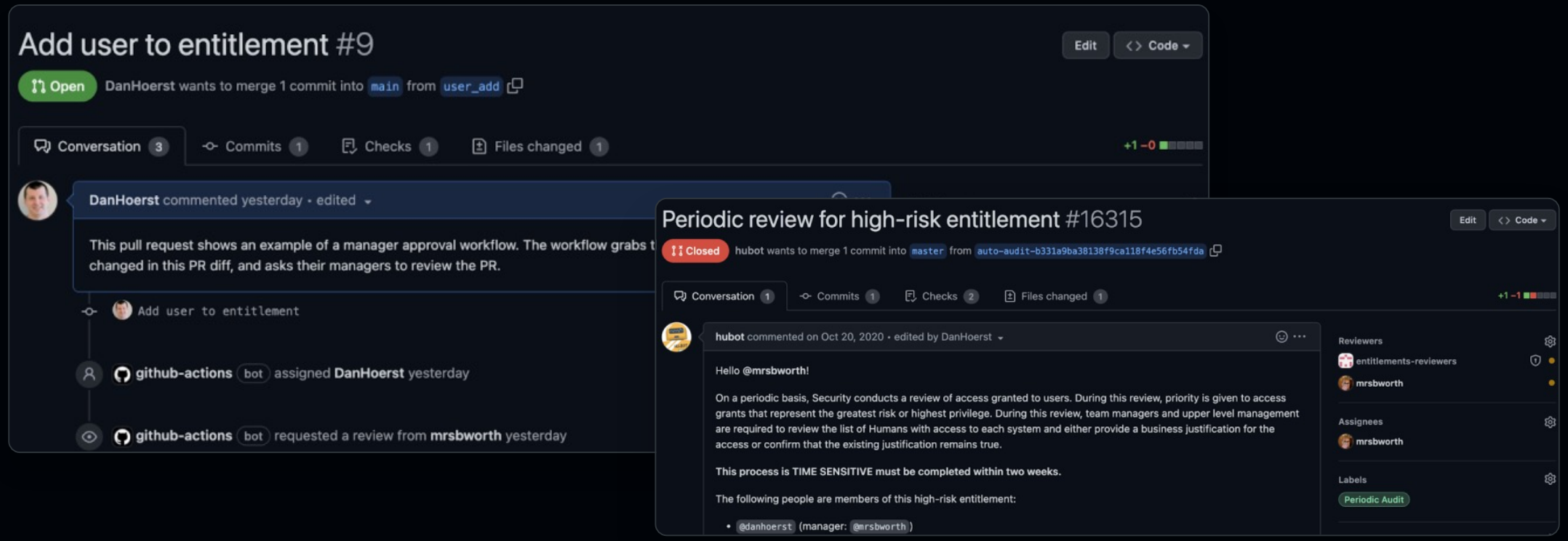
Microsoft ♥ GitHub

+

+ Semmle

GitHub
Advanced Security

GitOps + IAM


Add user to entitlement #9
Edit
Code
Open
DanHoerst wants to merge 1 commit into main from user_add
Conversation 3
Commits 1
Checks 1
Files changed 1
+1 −0
DanHoerst commented yesterday • edited
This pull request shows an example of a manager approval workflow. The workflow grabs t
changed in this PR diff, and asks their managers to review the PR.
Add user to entitlement
github-actions bot assigned DanHoerst yesterday
github-actions bot requested a review from mrsbworth yesterday
Periodic review for high-risk entitlement #16315
Edit
Code
Closed
hubot wants to merge 1 commit into master from auto-audit-b331a9ba38138f9ca118f4e56fb54fda
Conversation 1
Commits 1
Checks 2
Files changed 1
+1 −1
hubot commented on Oct 20, 2020 • edited by DanHoerst
Hello @mrsbworth!
On a periodic basis, Security conducts a review of access granted to users. During this review, priority is given to access grants that represent the greatest risk or highest privilege. During this review, team managers and upper level management are required to review the list of Humans with access to each system and either provide a business justification for the access or confirm that the existing justification remains true.
This process is TIME SENSITIVE must be completed within two weeks.
The following people are members of this high-risk entitlement:
@danhoerst (manager: @mrsbworth)
Reviewers
entitlements-reviewers
mrsbworth
Assignees
mrsbworth
Labels
Periodic Audit

Security at every step

Native, first party security by design to fix issues in minutes, not months

48%	Real-time fix Rate in the PR
72%	Fix rate in 28 days
22%	Productivity boost realized compared to traditional tools

Today →

That brings us to today

AI will define the developer experience


Security
Speed
Developers can’t just build a great product anymore
Continuous

How is AI changing development?

runtime.go | course.rb | time.js | IsPrimeTest.java

```go
package main

type Run struct {
    Time int // in milliseconds
    Results string
    Failed bool
}
```

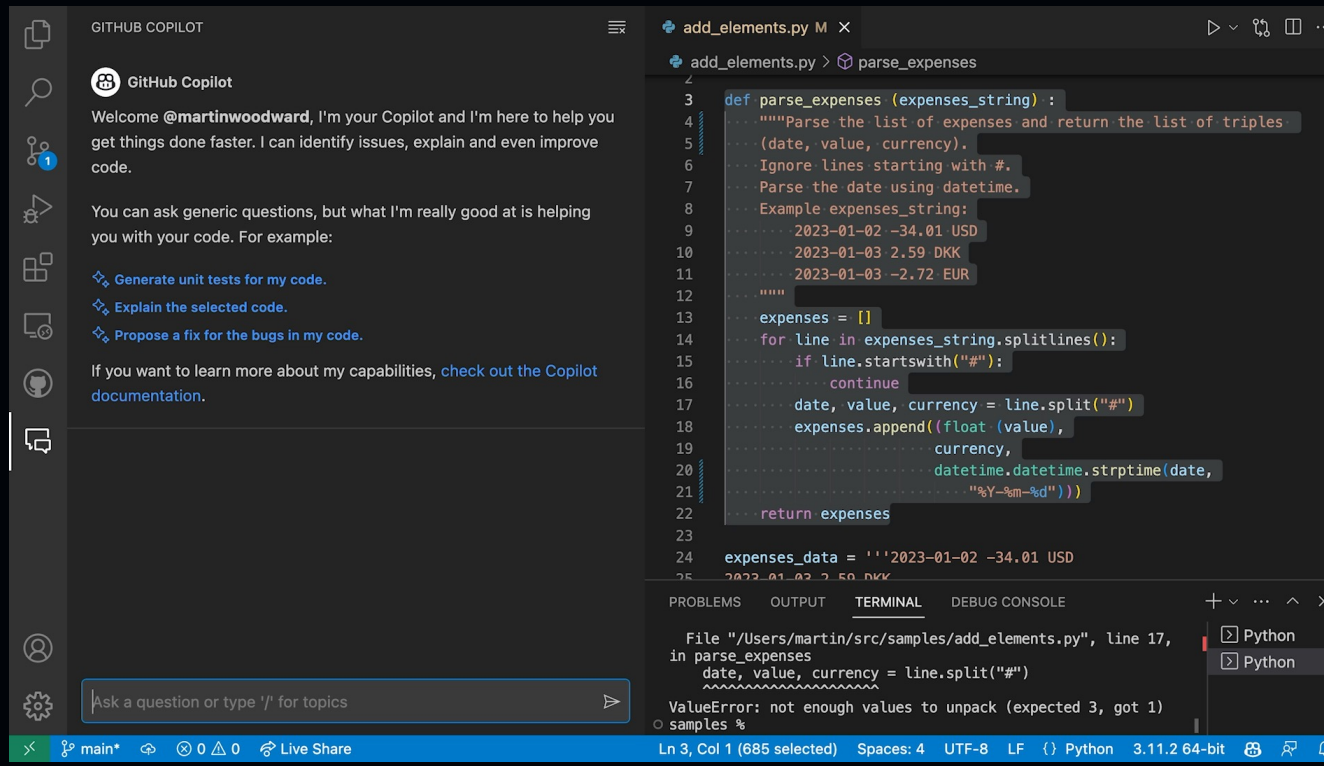
AI-based security vulnerability filtering

Code Security – Modeling

Security + Developers

Chat GPT

Code security - modeling



AI and Security

35%

Acceptance rate

46%

New code written by AI

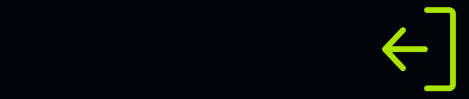
55%

Faster taskcompletion

75%

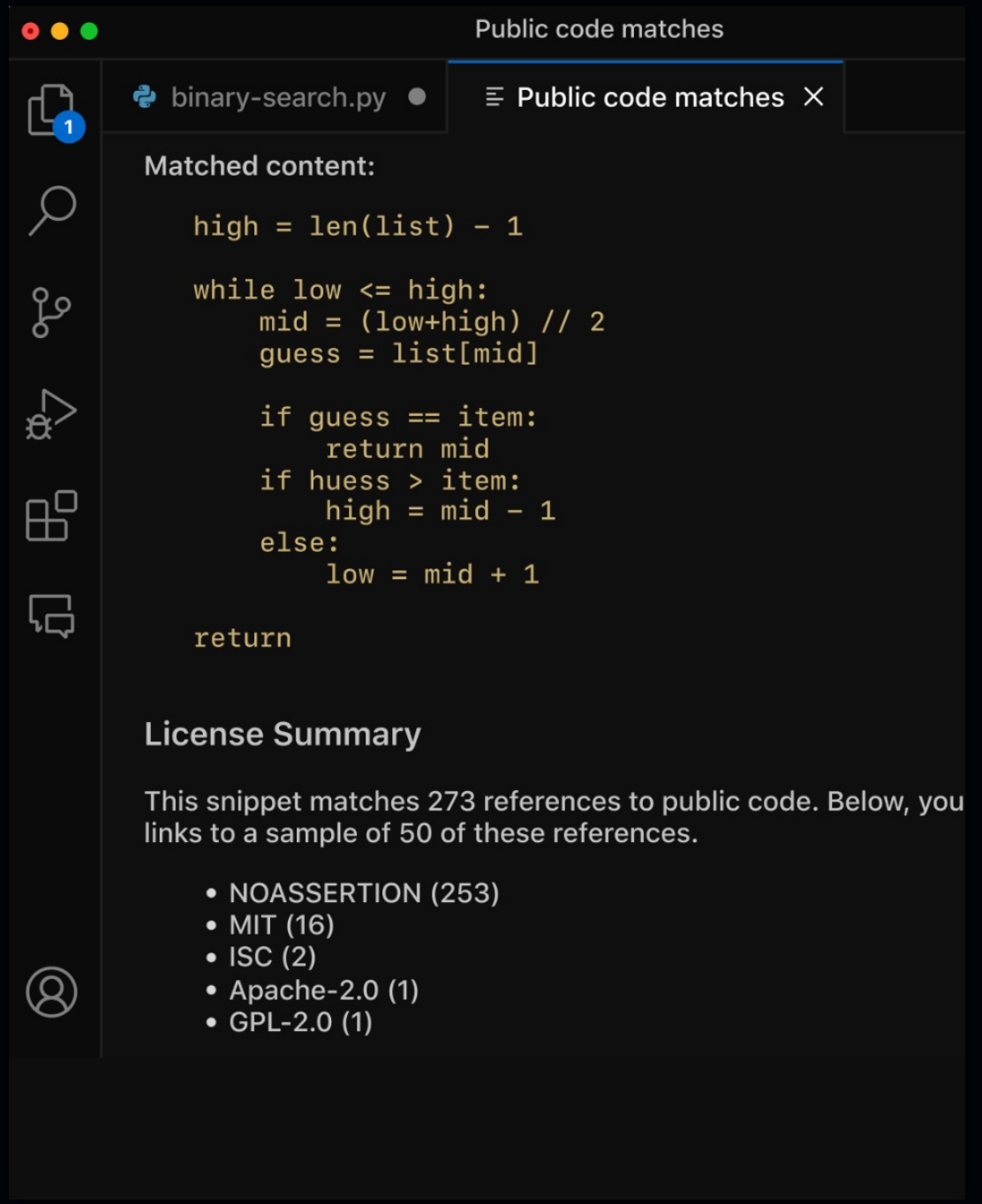
Developers more fulfilled

Intellectual Property



Intellectual Property

Intellectual Property



But...

How safe are they?

Common Concerns

Adoption

Should we wait till AI is more established?

Workforce

Will this hurt my team? Will they not have enough to do?

Emerging risks

Help, I’m looking for…

Thank you

@jacobdepriest

Jacob DePriest

VP, Deputy CSO