



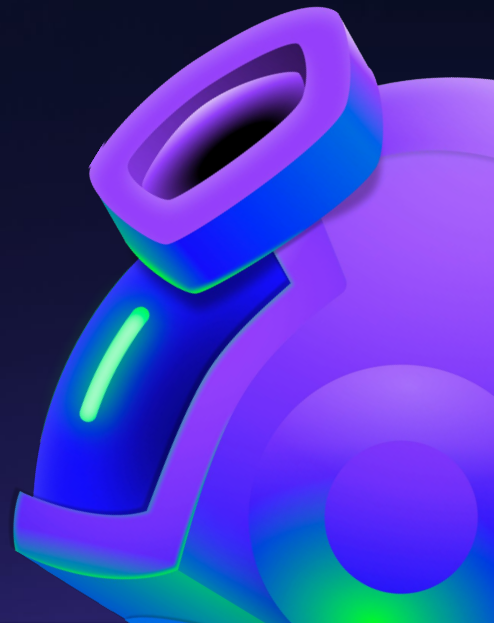
# GitHub Copilot & GitHub Advanced Security

- *a quick tour*

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



Karl Krukow  
krukow@github.com



## Speaker Bio



Karl Krukow

**Karl Krukow**

**Sr. Director, Software engineering, GitHub**

Code scanning team, part of GitHub Advanced Security

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

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

[krukow@github.com](mailto:krukow@github.com)

---





# The GitHub vision



A single  
integrated  
enterprise-ready  
platform



Security at  
every step of  
the workflow



Industry-best  
collaborative tools  
for developers

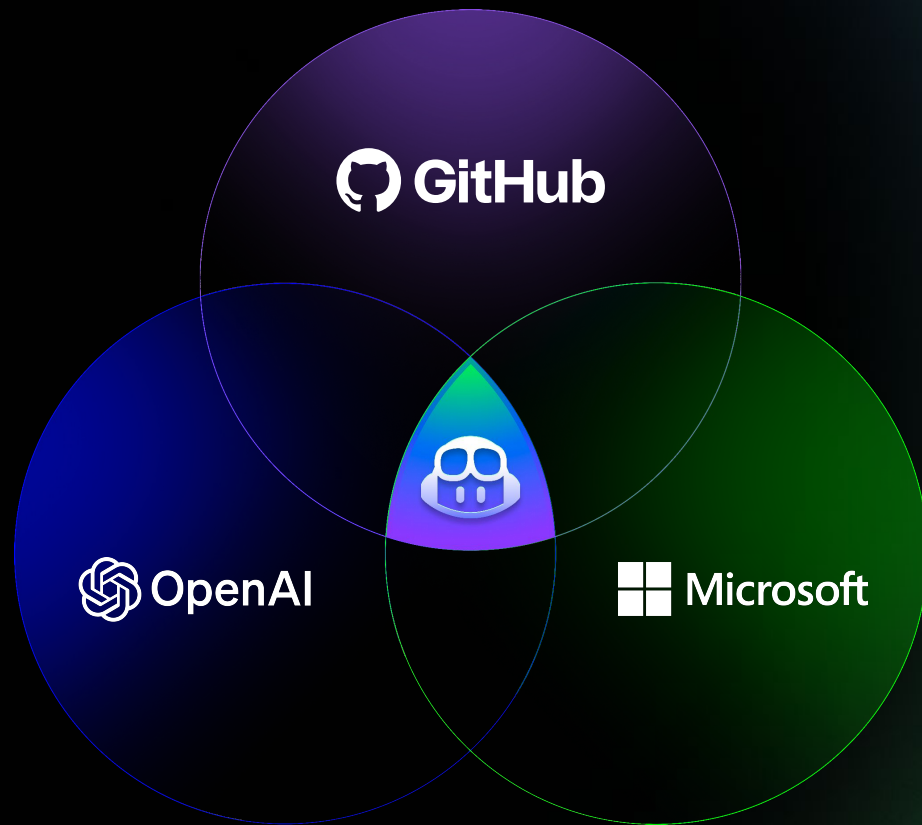


Powered  
By AI





Part of  
Microsoft,  
Partnering  
with OpenAI







# Our Agenda

01

**GitHub Copilot & Copilot Enterprise**

What, how, why?

02

**GitHub Advanced Security & CodeQL**

Find and prevent code security issues - an overview

03

***Autofix* powered by Copilot & CodeQL**

Fast and automated remediation of security risk

# Resources and Common questions

- [GitHub Copilot Trust center](#) - default entry point for security, privacy, and compliance questions
- [Contractual protection](#):
  - GitHub has created [a duplication detection filter](#) to detect and suppress GitHub Copilot suggestions that contain code snippets that match public code on GitHub.
  - tldr: **turn blocking on** ⇒ **GitHub provides indemnity (read details)**
- [How copilot handles data](#):
  - Copilot for Business does not retain any prompts for training its models or any other development of Microsoft or GitHub products.  
*Prompts are discarded once a suggestion is returned.*
- [Tips for a successful rollout of GitHub Copilot](#)



# GitHub Copilot - What is it?

GitHub Copilot is the world's most widely adopted AI developer tool.

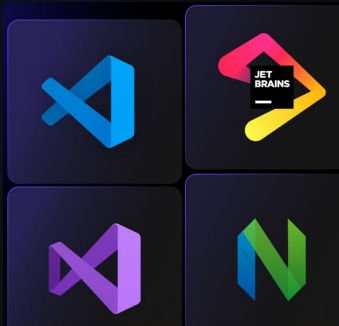


**AI-powered  
code suggestions  
in real time**



**context-aware  
conversations  
with AI assistant**

In the  
**IDE and  
Terminal**

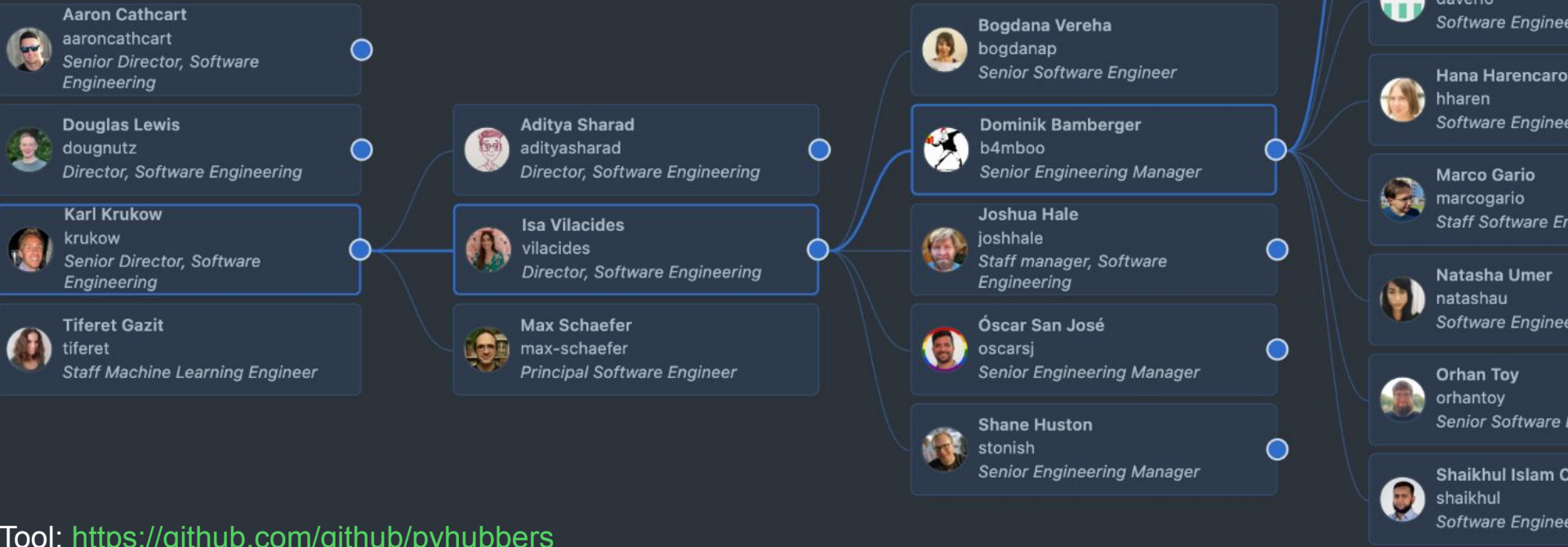




# Demo



# Our engineering organization



Tool: <https://github.com/github/pyhubbers>



# Global shift in the way software is developed.

Copilot enables  
55% faster  
coding and  
15% higher code  
quality



50,000+  
businesses  
building software  
with Copilot

```
16 def test_parse_expenses_with_comments(self):
17     expenses_string = '# This is a comment\n2023-01-02'
18     expected_output = [(datetime.datetime(2023, 1, 2),
19     self.assertEqual(parse_expenses(expenses_string),
20
21
22
23
24
25
26
27
28
29
30
31
32
```

Analyze and debug

Ask a question or type '/' for topics



# A 6-month study of 450 Accenture developers on the impact of GitHub Copilot



## Activity

94%

Reported staying in the flow

90%

Spent less time looking for information



## Productivity

90%

Reported writing better code

88%

Of the code suggested by Copilot retained



## Efficiency

50%

More builds

84%

Increased in successful builds



## Satisfaction

96%

Successful on day one

90%

More fulfilled





# Copilot Enterprise for an AI-powered software development lifecycle.

From the  
IDE, CLI,  
and  
mobile



To the  
Platform



# Tailor Copilot to your organization's repositories and knowledge base.



## Discover

Does code already exist for this?

Help! I need step-by-step instructions.



## Explain

What does this code do?

Why is this important?



## Analyze


What needs my attention?

Does anything here use anti-patterns?



- The submission process itself is handled by the `TalkSubmitView` class in `views.py`. This is a `CreateView` which requires the user to be logged in (`LoginRequiredMixin`). The form asks for 'title', 'abstract', and 'track' fields for a talk. Once the form is filled out and submitted, the talk is associated with the logged-in user and saved to the database ([source](#)).

Is there anything else you'd like to know about this process?

3 references 



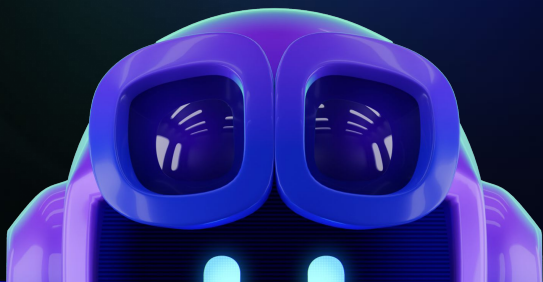
Is it OK |



General availability

# Copilot Enterprise

Bring domain expertise from your code and knowledge to Copilot Chat.



Coming soon

# Custom models

Add knowledge of SDKs, APIs, and under-represented languages to the Copilot code completion model.

+ Add-on

Early 2025

# Plugins

Integrate your preferred third-party tools, databases, and services with Copilot.



# GitHub Advanced Security

# GitHub Advanced Security



secret scanning



supply chain



code scanning



security overview

**free** *for public repos to help secure OSS!*





# Code scanning provides a security review of every code change

The screenshot shows a GitHub pull request interface. At the top, there are navigation tabs for 'Code', 'Issues', 'Pull requests', 'Actions', 'Projects', and 'Wiki'. Below these, there are summary statistics: 'Conversation 1', 'Commits 1', 'Checks 2', and 'Files changed 7'. A comment from 'greysteil' is visible, stating: 'Adds an email confirmation flow. We'll include a token in the emails we send users, and check for it when they click the "verify your email" link.' Below the comment, a code change is shown for 'Basic confirmation email flow'. A 'github-code-scanning' bot comment is highlighted with a red box, indicating a 'Check failure' for 'Code scanning / CodeQL'. The alert message is: 'Database query built from user-controlled sources (High)'. Below this, it says 'This query depends on a user-provided value.' and provides a 'Show more details' link. At the bottom of the alert, there are 'Show paths' and 'Dismiss alert' buttons. The code snippet shown is from 'server/apps/routes/auth.js' and includes the following lines: 'router.get('/verify', async (req, res) => {', 'const token = req.query.t;', and 'const user = await User.findOne({ token });'.





# CodeQL

GitHub's powerful semantic code analysis engine which powers GitHub code scanning



# CodeQL

*QL is the powerful object oriented, logic programming query language that underlies CodeQL.*

*Understands program structure and performs advanced data flow and taint-tracking analysis*

<https://codeql.github.com/>



## ***Your code as a database***

*Run database queries to find vulnerable code*



## ***Comes with batteries included***

*25% growth in out-of-the-box security queries since last year, finding more CWEs*



## ***Low false-positive rate***

*High signal-to-noise ratio to keep developers happy and engaged*



## ***Extensible with custom queries***

*Find custom code patterns or data flows in your code-base - find security or code quality issues*



## Found means fixed: autofix powered by Copilot and CodeQL

Following CodeQL analysis, autofix will propose a fix for new alerts. These remediation suggestions are then posted as a code suggestion on the PR.

The remediation suggestions give developers precise and actionable feedback on where issues exist in the codebase and what changes need to be made to fix them. Developers can commit the proposed fix to effortlessly remediate vulnerabilities, all without leaving their workflow

The screenshot shows a GitHub pull request for a repository named 'dsp-testing / auto-fix-ui-demo'. The pull request title is 'A simple example of an XSS vulnerability #7'. A comment from 'orhantoy' includes a link to a GitHub repository: 'https://github.com/github/codeml-autofix/tree/main/cocofix/examples/synthetic-xss'. Below the comment, a CodeQL alert is displayed for 'index.js'. The alert title is 'Reflected cross-site scripting (Medium)'. The alert description states: 'Cross-site scripting vulnerability due to a user-provided value.' The code snippet shows the following lines:

```
1 + const express = require('express');
2 +
3 + const app = express();
4 + app.get('/', (req, res) => res.send('Hello, ${req.query.name}!'));
```

The alert includes a 'Check warning' icon, a 'Code scanning / CodeQL' label, and a 'Show more details' link. There are also 'Show paths' and 'Dismiss alert' buttons at the bottom of the alert.



# Demo



# Thank You!

01

## GitHub Copilot & Copilot Enterprise

Happier and more productive developers

02

## GitHub Advanced Security & CodeQL

Detect and Prevent security issues in your applications with every change

03

## *Autofix* powered by Copilot & CodeQL

Automatically fix security issues to reduce risk

## Speaker Bio



Karl Krukow

Sr. Director, Software engineering

Code scanning,

GitHub Advanced Security

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

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

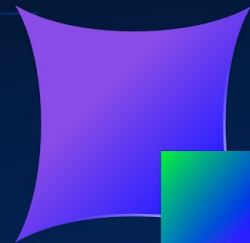
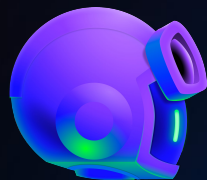
[krukow@github.com](mailto:krukow@github.com)

---





# Thank You!







# Appendix



# Flight Reports

...



Trying to code in an unfamiliar language by googling everything is like navigating a foreign country with just a phrasebook. **Using GitHub Copilot is like hiring an interpreter.**

Harri Edwards // Open AI



# Flight Reports

...




A tool like GitHub Copilot is so impactful at large companies because suddenly engineers can make impactful changes to other developers' code with little previous exposure.

Severin Hacker // CTO, Duolingo





# Flight Reports

 **swyx**  
@swyx

By far the greatest benefit of using @Github Copilot so far is I now don't have to be forced to document my code.

I actively \*want\* to write great comments, because when I do, I get the dopamine hit of a good Copilot suggestion.

7:51 PM · Oct 12, 2022 from Puerto Vallarta, Jalisco

21 Retweets 3 Quote Tweets 338 Likes

 **Danny Postma**  
@dannypostmaa

AI is doing 80% of my coding – the future looks brighter than ever! 😁

```
90 methods: {
91   async fetch () {
92     // |
93
94
95     this.test = await this.$axios.$get('/admin/analytics', {
96       params: {
97         startDate: this.date.start,
98         endDate: this.date.end
99       }
100     })
101     this.isLoading = false
102   }
103 }
104
```

0:17 493.5K views

4:37 PM · Dec 1, 2022


1,161 Retweets 187 Quote Tweets 9,969 Likes

 **John Skoubourdis**  
@scoumbourdis

GitHub Copilot is like giving a programmer a super power 🦹

11:41 PM · Jun 2, 2022

1,579 Retweets 137 Quote Tweets 22.6K Likes

 **@willman@xoxo.zone**  
@willmanduffy

You win this round Copilot

```
updateMyselfMutationVari
Name: 'Bob',
ame: 'Builder',
```

5:01 PM · Jun 14, 2022

50 Retweets 3 Quote Tweets 780 Likes

 **JD Ross** ✓  
@justindross

Some of our engineers just told me they'd estimate 40% of the lines of code they produce are now written by the Github CoPilot AI

6:13 PM · Oct 19, 2022

386 Retweets 159 Quote Tweets 5,220 Likes

 **Alex MacCaw** ✓  
@maccaw

One of the best uses of GitHub CoPilot is autocompleting your tests.

At this point it's writing the majority of my tests.

5:55 PM · Oct 29, 2022

20 Retweets 3 Quote Tweets 307 Likes