

100M+ Developers, Security, and AI

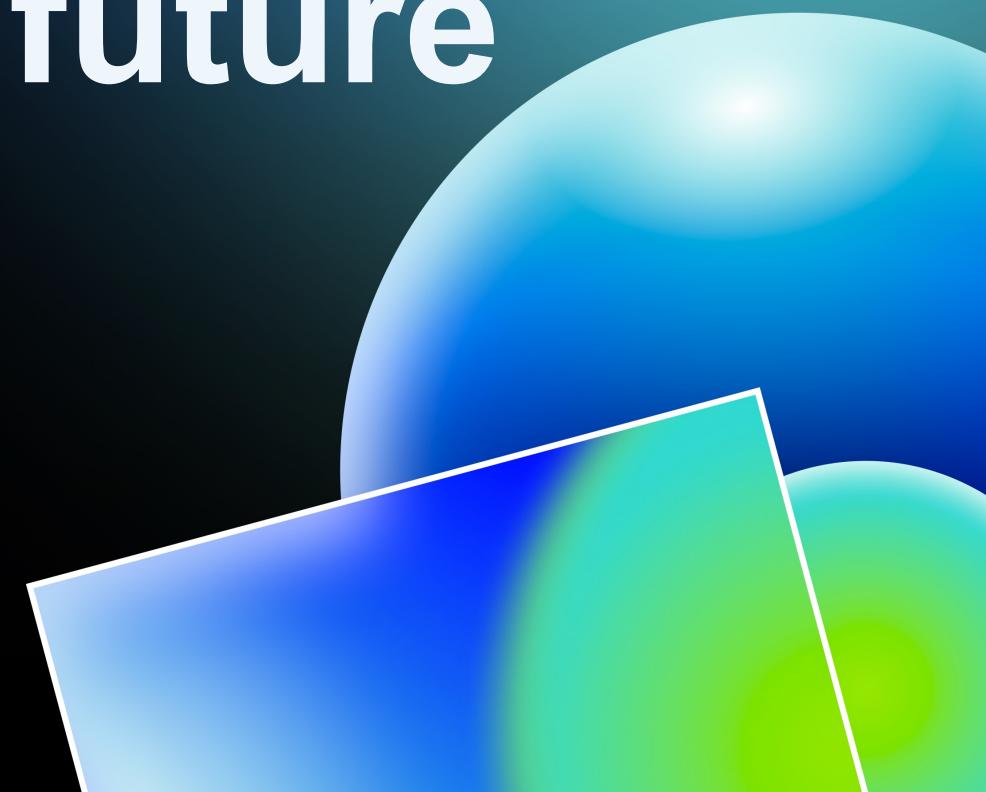
# My journey from DevOps to an AI-assisted future



@jacobdepriest

Jacob DePriest

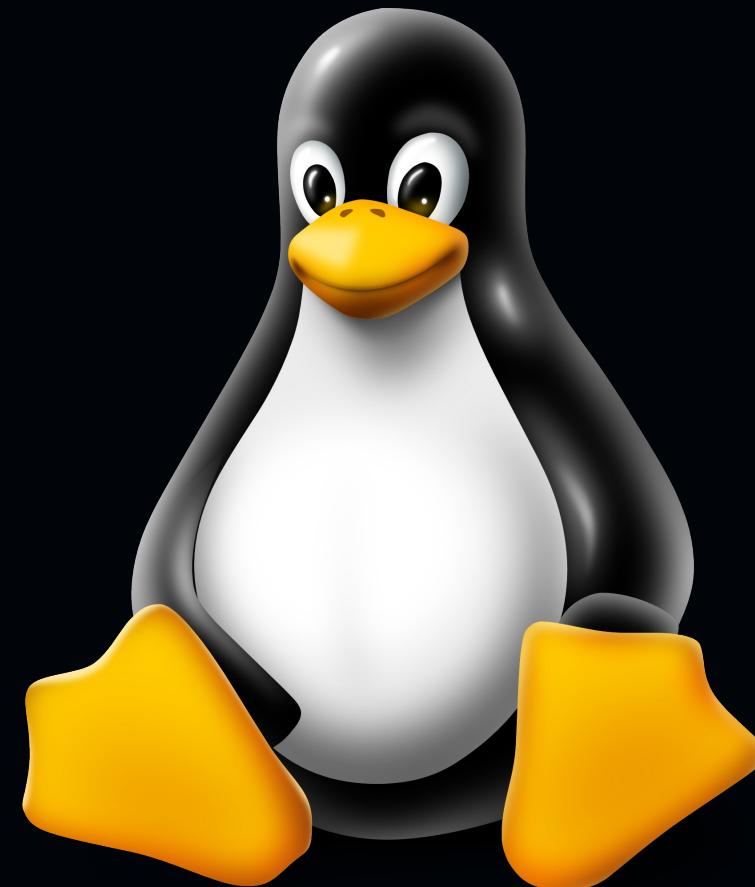
VP, Deputy CSO



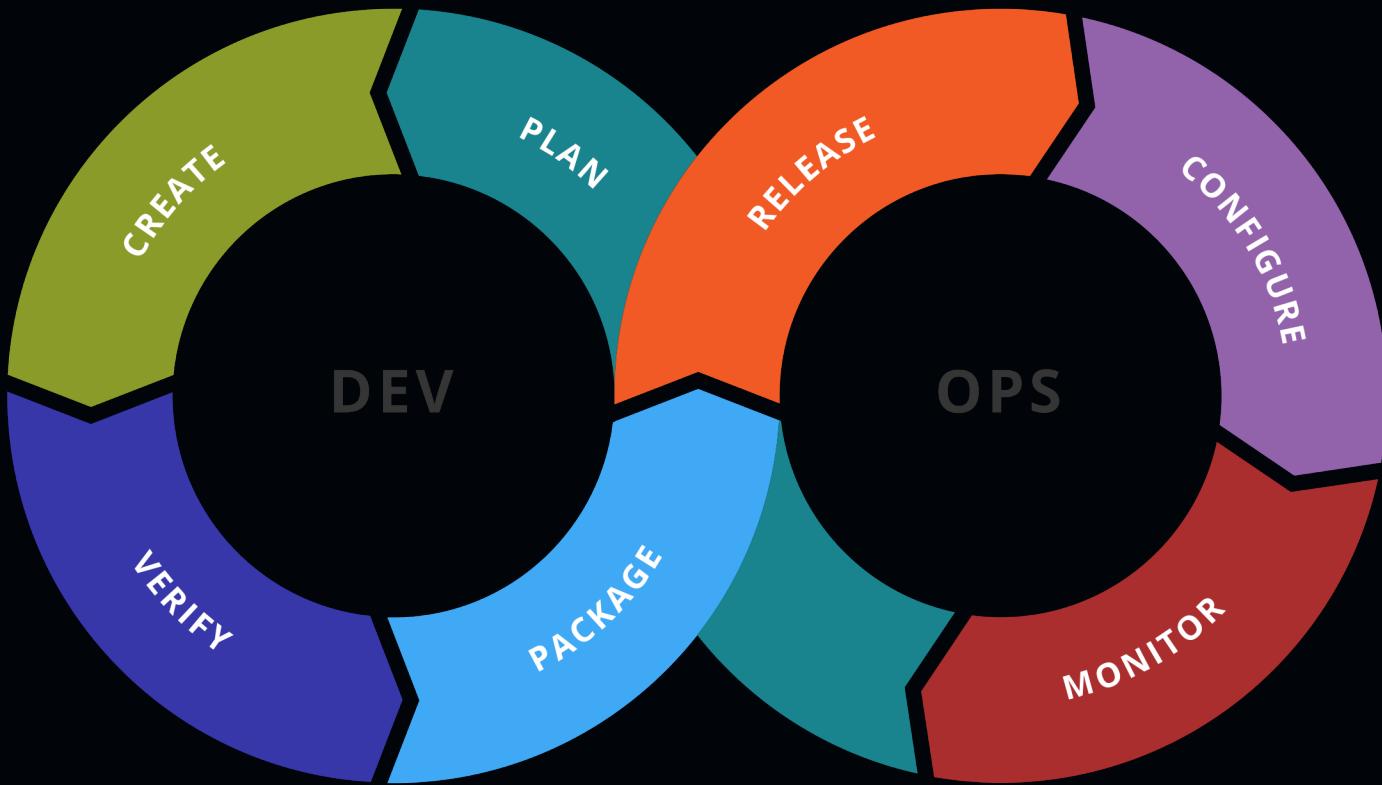
# How'd we get here?



# Open Source Software



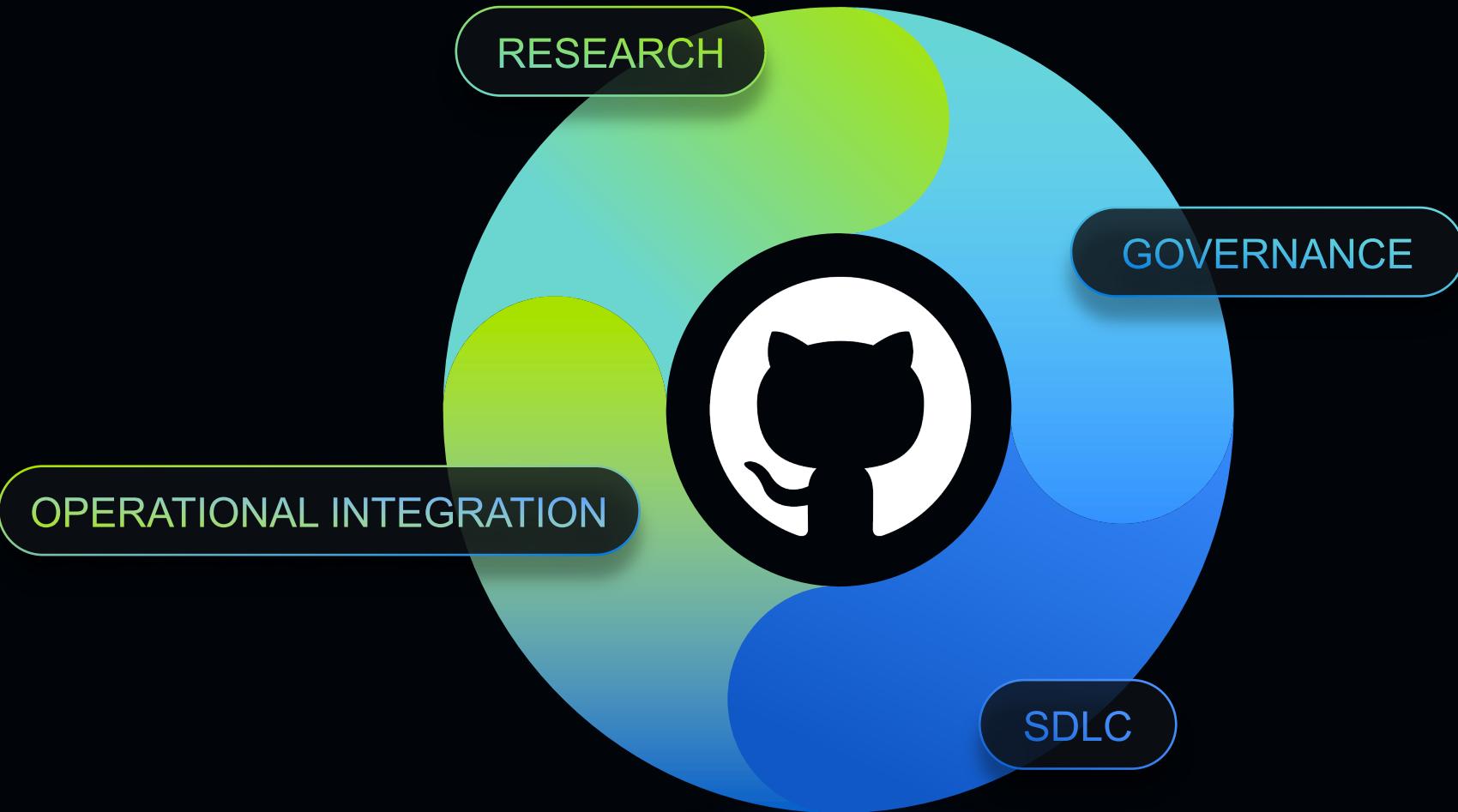
# DevX



# Unclass Work & Cyber Collaboration

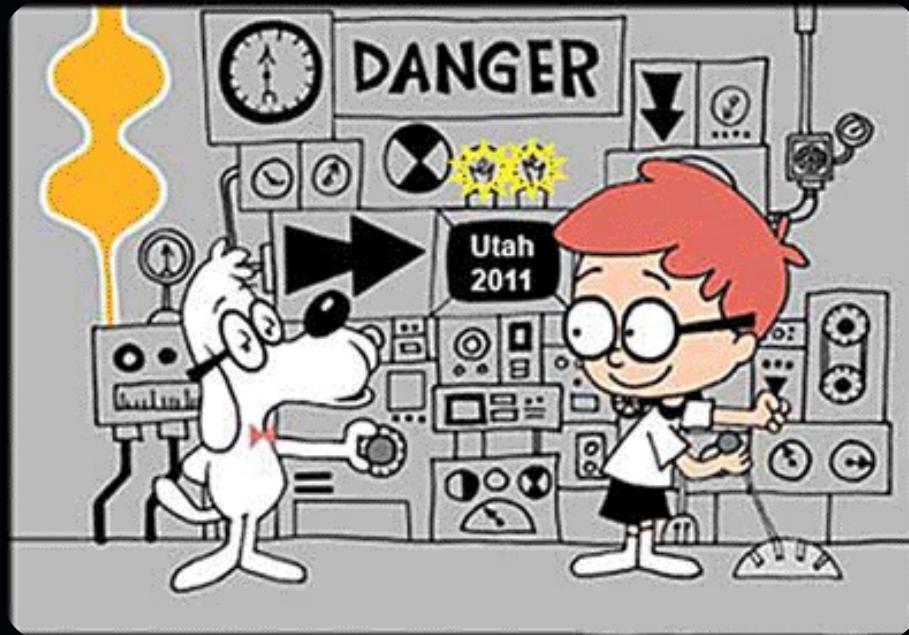






# DevSecOps at GitHub





GitHub

Then  
& now

2011 - 2012



2M  
Repositories



WORKING ASYNCHRONOUSLY:



github  
SOCIAL CODING

NO MEETINGS • NO DEADLINES • NO MANAGERS

pull requests  
+ branching

Optimize for ^ Happiness

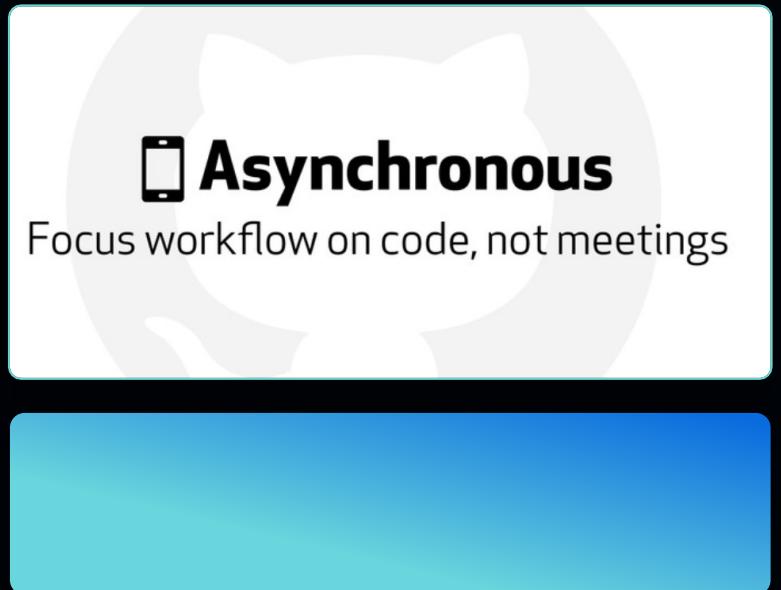
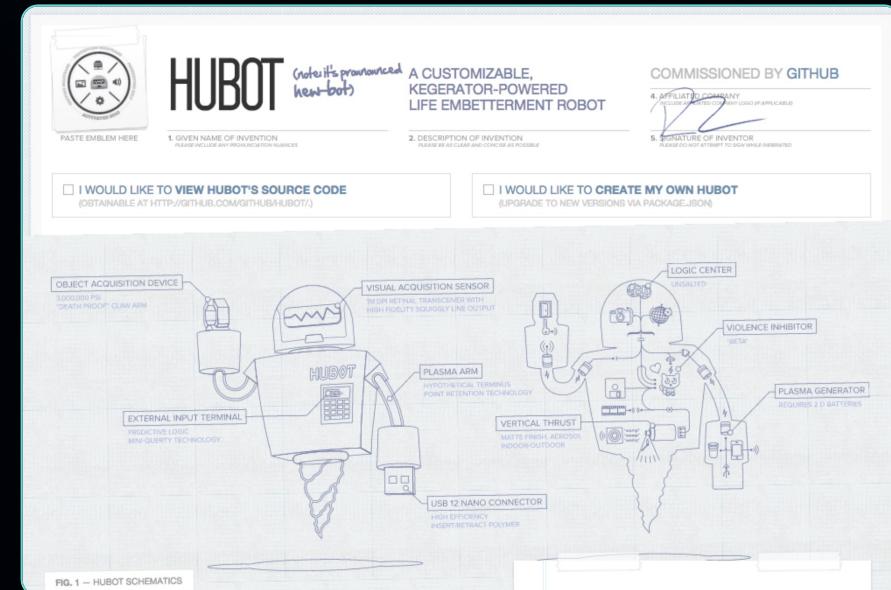
developer



2014 - 2018

21M

Repositories



## A typical deployment flow

Development → Staging → Production



2018 - 2022



**100M**

Repositories



Microsoft



GitHub



+



+ Semmle

GitHub  
Advanced Security

# GitOps + IAM

The screenshot displays two GitHub pull requests illustrating a workflow for managing access grants:

**Pull Request #9: Add user to entitlement**

- Status:** Open
- Author:** DanHoerst
- Description:** DanHoerst wants to merge 1 commit into `main` from `user_add`.
- Activity:** Conversation (3), Commits (1), Checks (1), Files changed (1).
- Comment by DanHoerst:** This pull request shows an example of a manager approval workflow. The workflow grabs the users that have been added in this PR diff, and asks their managers to review the PR.
- Actions:** Add user to entitlement, Assignments (github-actions bot assigned DanHoerst), Request review (github-actions bot requested a review from mrsbworth).

**Pull Request #16315: Periodic review for high-risk entitlement**

- Status:** Closed
- Author:** hubot
- Description:** hubot wants to merge 1 commit into `master` from `auto-audit-b331a9ba38138f9ca118f4e56fb54fda`.
- Activity:** Conversation (1), Commits (1), Checks (2), Files changed (1).
- Comment by hubot:** 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.
- Text:** This process is **TIME SENSITIVE** must be completed within two weeks.
- Text:** 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?



AI-based security  
vulnerability filtering



Code Security –  
Modeling

A screenshot of a code editor interface showing a file named "runtime.go". The code defines a struct "Run" with fields: Time (int), Results (string), and Failed (bool). The code editor also shows tabs for other files: "course.rb", "time.js", and "IsPrimeTest.java".

```
1 package main
2
3 type Run struct {
4     Time int // in milliseconds
5     Results string
6     Failed bool
7 }
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
```

# Security + Developers



Chat GPT



Code security - modeling

GITHUB COPILOT

GitHub Copilot

Welcome @martinwoodward, I'm your Copilot and I'm here to help you get things done faster. I can identify issues, explain and even improve code.

You can ask generic questions, but what I'm really good at is helping you with your code. For example:

- Generate unit tests for my code.
- Explain the selected code.
- Propose a fix for the bugs in my code.

If you want to learn more about my capabilities, [check out the Copilot documentation](#).

add\_elements.py M X

```
def parse_expenses (expenses_string) :  
    """Parse the list of expenses and return the list of triples  
    (date, value, currency).  
    Ignore lines starting with #.  
    Parse the date using datetime.  
    Example expenses_string:  
        2023-01-02 -34.01 USD  
        2023-01-03 2.59 DKK  
        2023-01-03 -2.72 EUR  
    """  
    expenses = []  
    for line in expenses_string.splitlines():  
        if line.startswith("#"):  
            continue  
        date, value, currency = line.split("#")  
        expenses.append((float(value),  
                        currency,  
                        datetime.datetime.strptime(date,  
                            "%Y-%m-%d")))  
    return expenses  
expenses_data = '''2023-01-02 -34.01 USD  
2023-01-03 2.59 DKK
```

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE

File "/Users/martin/src/samples/add\_elements.py", line 17,  
in parse\_expenses  
 date, value, currency = line.split("#")  
ValueError: not enough values to unpack (expected 3, got 1)

samples %

Ln 3, Col 1 (685 selected) Spaces: 4 UTF-8 LF Python 3.11.2 64-bit

# AI and Security



**35%**

Acceptance rate

**46%**

New code written by AI

**55%**

Faster task completion

**75%**

Developers more fulfilled



# Intellectual Property



# Intellectual Property

# Intellectual Property



Public code matches

binary-search.py • Public code matches X

Matched content:

```
high = len(list) - 1

while low <= high:
    mid = (low+high) // 2
    guess = list[mid]

    if guess == item:
        return mid
    if guess > item:
        high = mid - 1
    else:
        low = mid + 1

return
```

License Summary

This snippet matches 273 references to public code. Below, you links to a sample of 50 of these references.

- NOASSERTION (253)
- MIT (16)
- ISC (2)
- Apache-2.0 (1)
- GPL-2.0 (1)

# 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

