Shift Left on Security with GitHub and Azure DevOps

Randy Pagels
DevOps Architect | Xpirit USA

Xebia | Xpirit

Microsoft Solutions Partner

GitHub Verified Partner

Let's connect

Randy-Pagels

@RandyPagels

PagelsR

https://xpirit.com

Randy Pagels

DevOps Architect

rpagels@xpirit.com

GitHub Universe 2023

Save the Date
November 8-9

Beyond Code: Global developer event!

November 8-9, San Francisco, CA + streaming on https://www.githubuniverse.com/

On Demand
On demand sessions will help you dive deeper.

Interactive
Get hands on with the people who write the code.

100+ Speakers

85+ Sessions

3 Tracks

Xebia | Xpirit

The State of Security Today

Security Incidents

- **2014:** **Healthcare.gov** suffered a data breach that exposed sensitive information of around 75,000 individuals due to a misconfiguration in the website's code.
- **2016:** **Zocdoc** healthcare appointment booking platform faced a security vulnerability that allowed unauthorized access to patient data, including names, email addresses, and appointment details.
- **2017:** A vulnerability found on **Equifax** servers allows hackers to execute malicious code remotely. 143 million records, 209,000 credit card numbers.
- **2018:** Hackers breached **Marriott Hotel** systems. Compromised 500 million users and exposes data records for 327 million guests.
- **2019:** **Experian Health** experienced a data breach that exposed personal and medical information of millions of patients. The breach occurred due to an unsecured Elasticsearch database used by the company.
- **2021:** **Log4j** vulnerability discovered. Millions of servers at risk due to popularity of Logging framework. Vulnerability gives hackers complete control over some applications
- **2023:** 38TB of data accidentally exposed by **Microsoft** AI researchers on a GitHub repository, including over 30,000 internal Microsoft Teams messages – all caused by a misconfigured SAS token.

4 years

On average, vulnerabilities go undetected for four years before being identified.

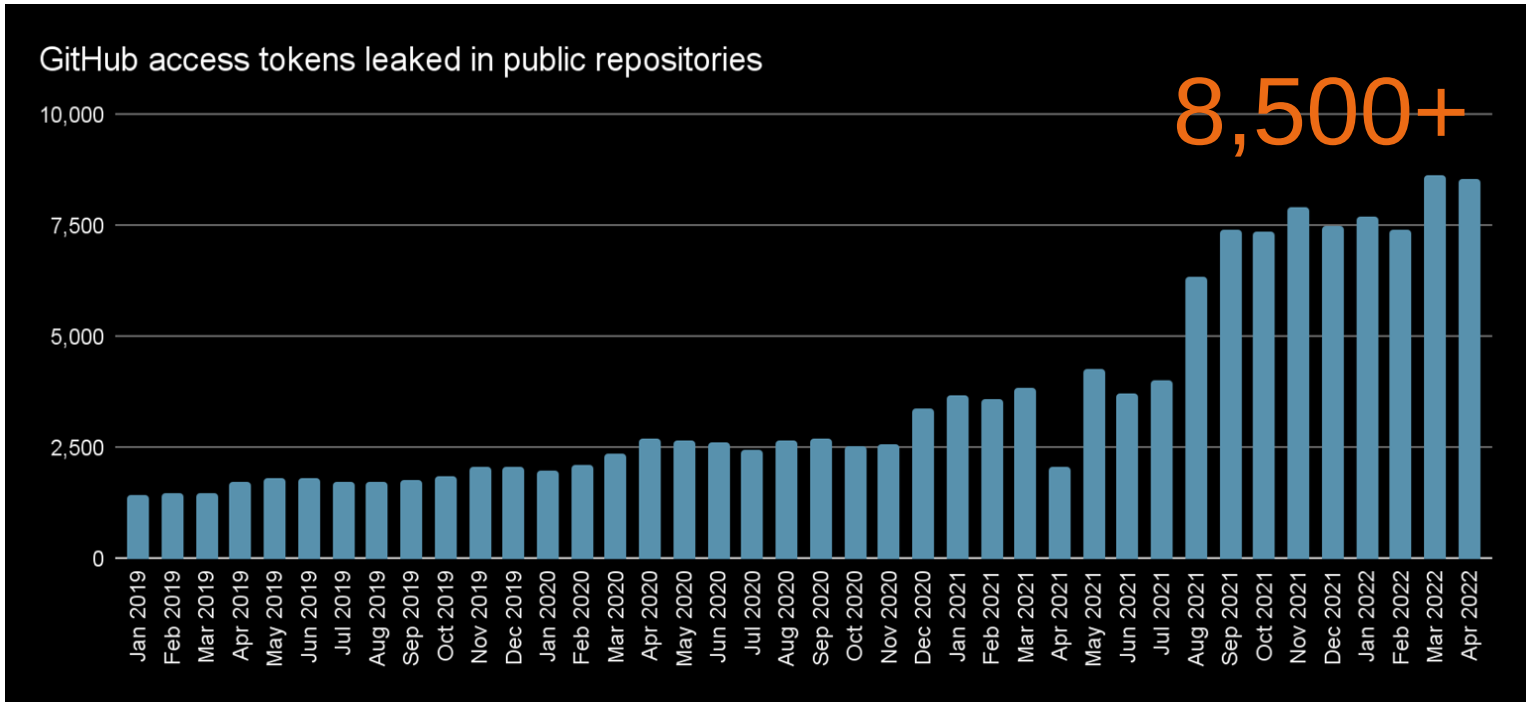
7 years

Sometimes, even longer than that:

- Log4j was vulnerable for ~7 years

Leaked Secrets

We’re seeing more credential leaks than ever

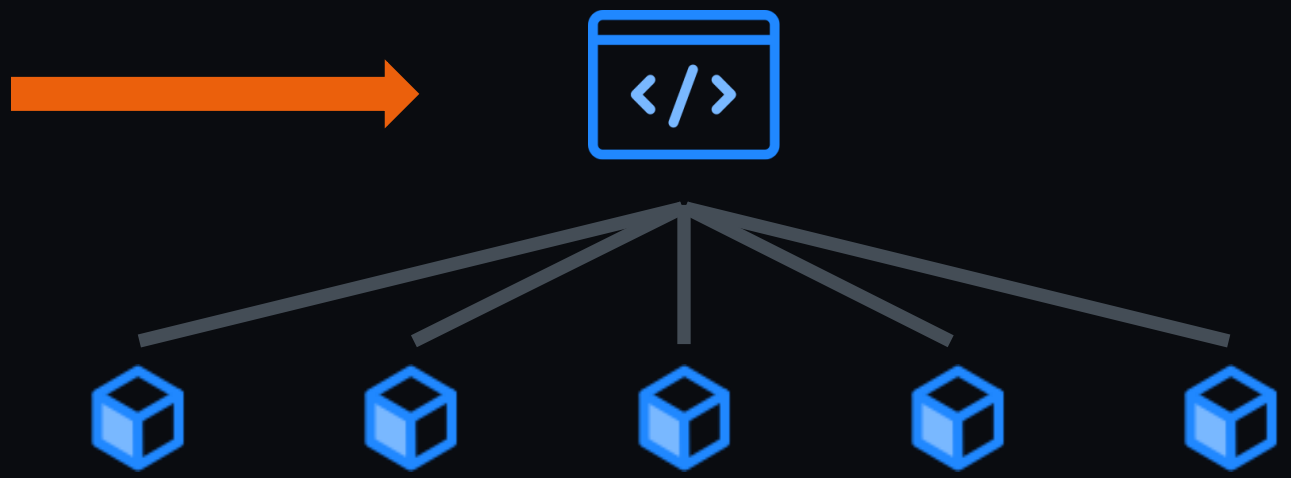


Source: GitHub data

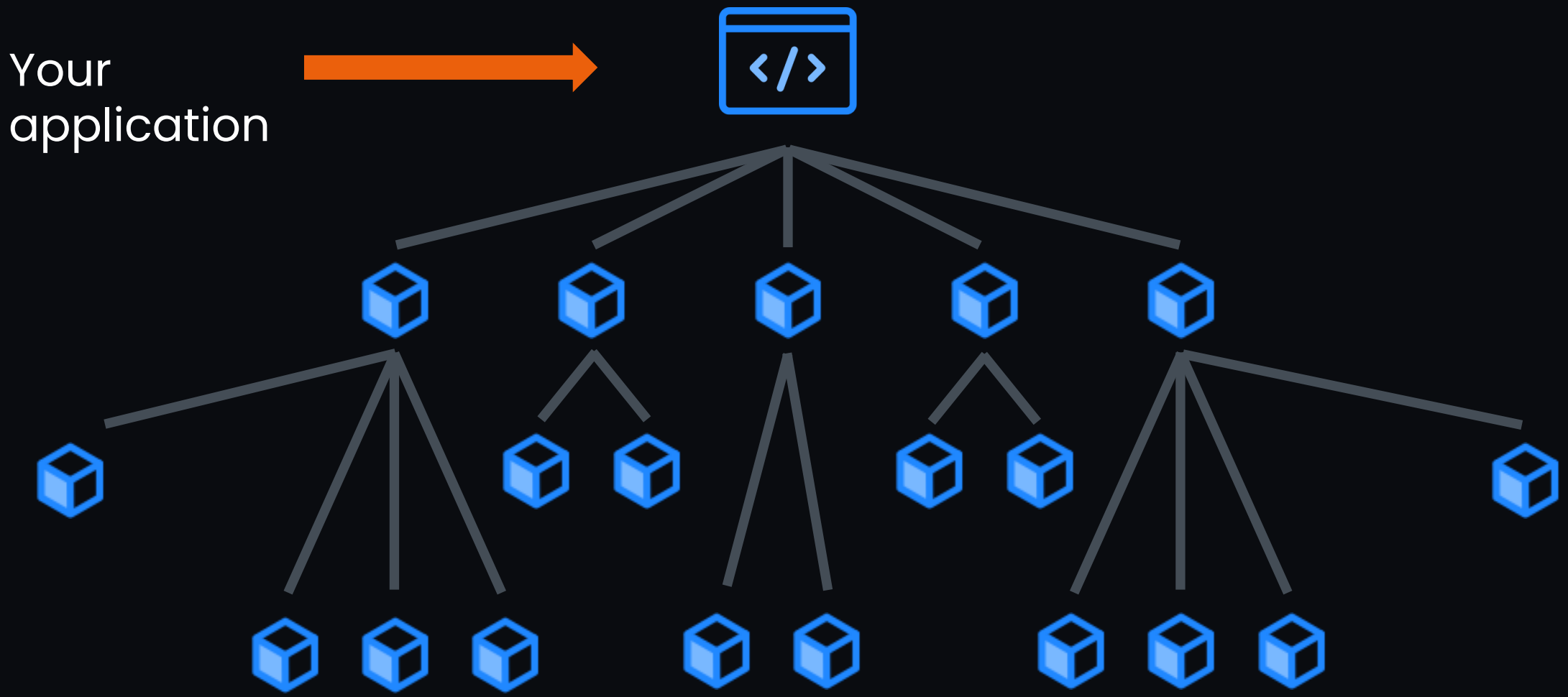
Secret Leaked exposing 38 TB of Data

80-90% of all code in distributed applications is Open Source

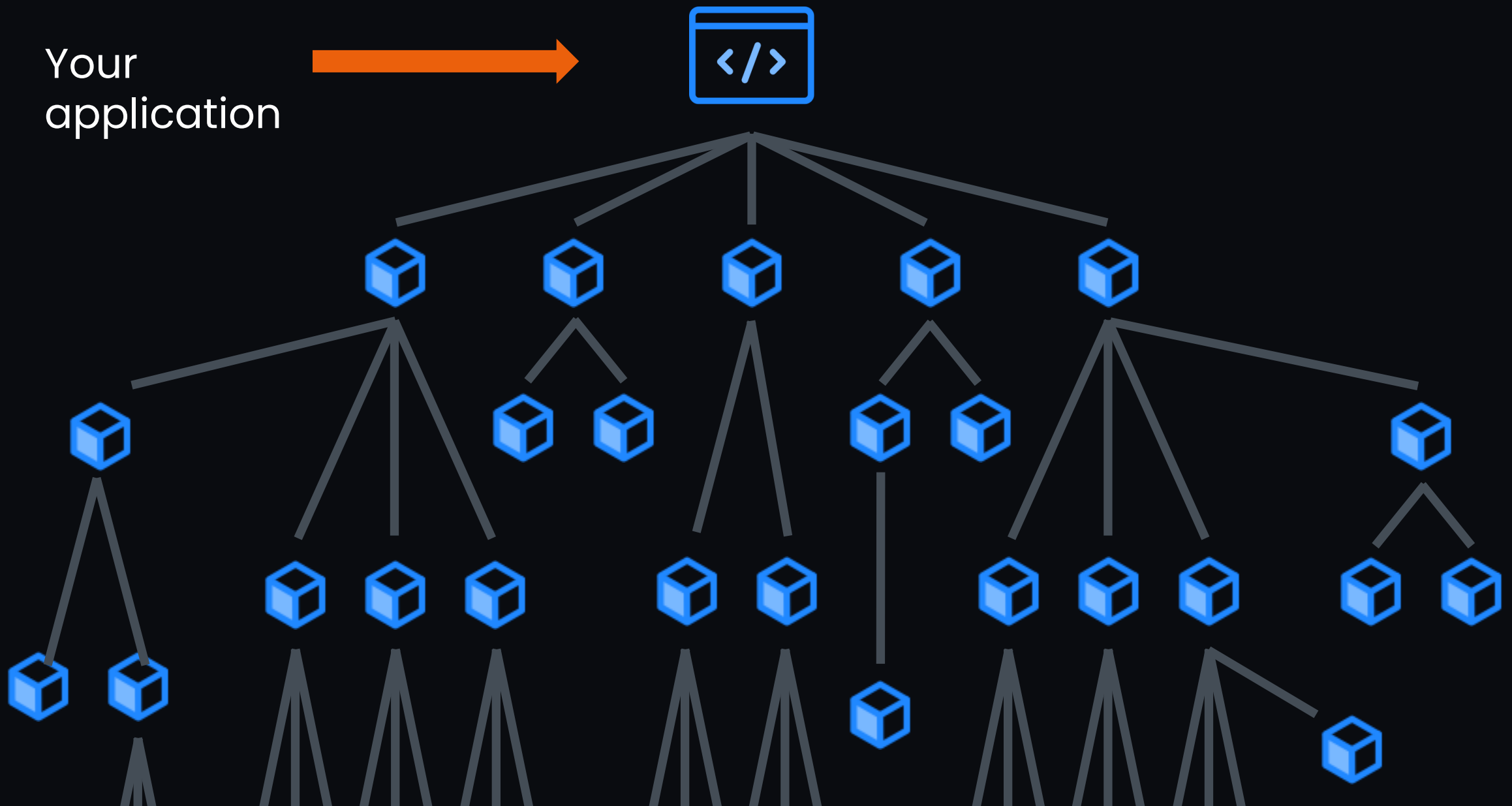
Your application

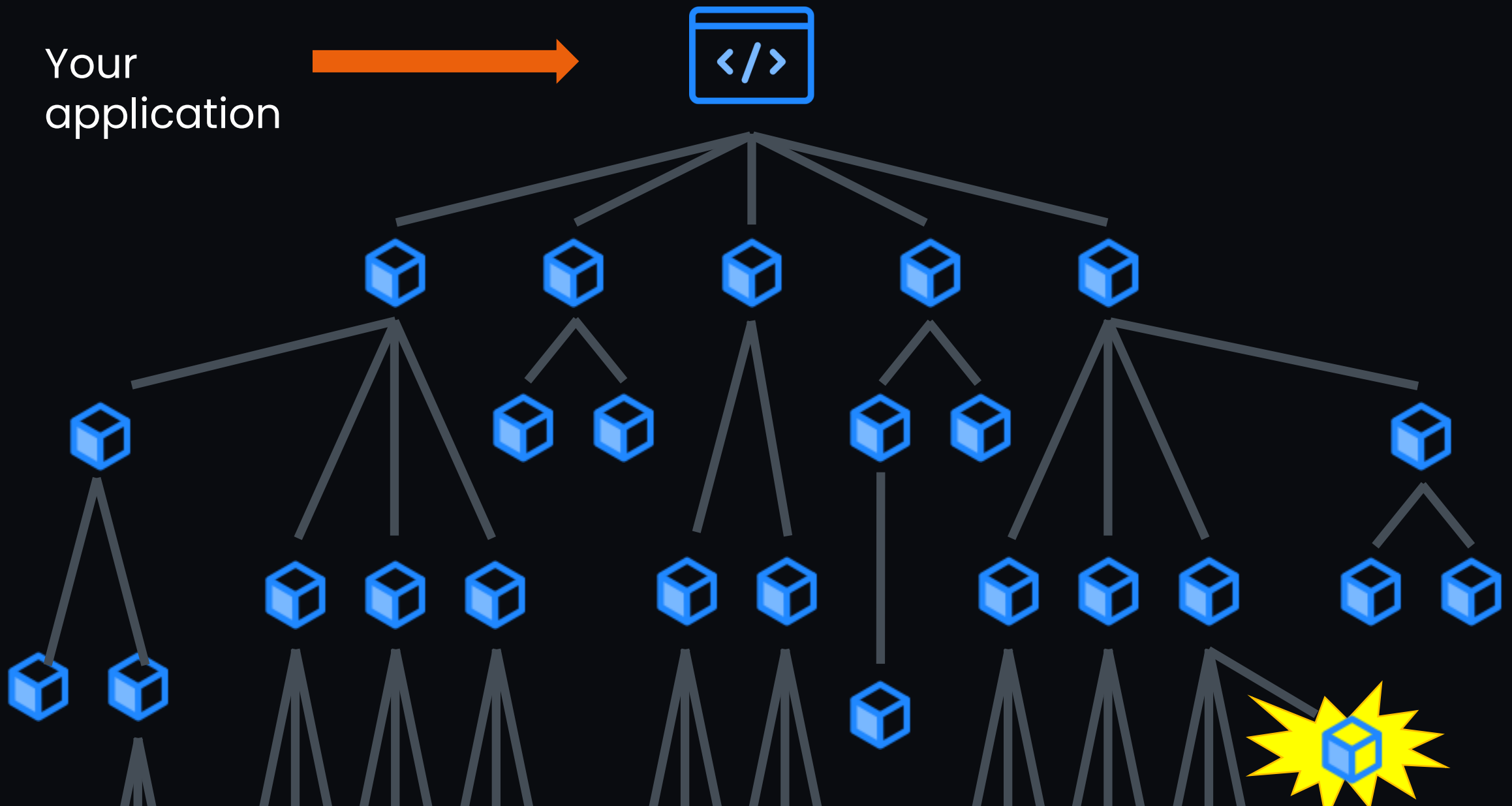


Dependency Chain starts with Top-Level Dependencies



Supply Chain of Dependencies


Your
application


Your
application


180+ days
Mean time to remediate (MTTR)
Industry norm

Mistakes happen

Some of those become a security risk!

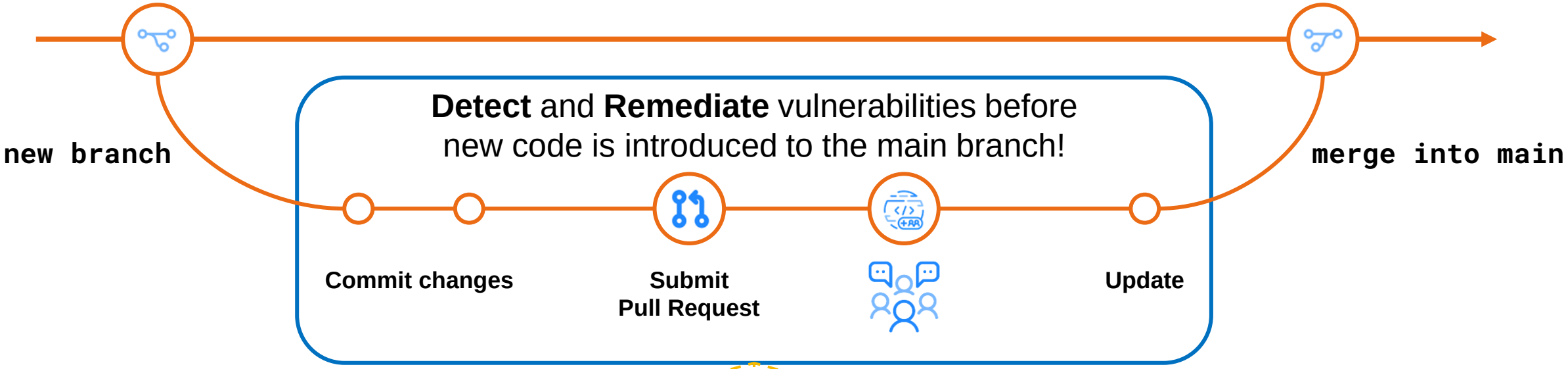
GitHub Advanced Security

GitHub believes that making this shift requires a developer-first approach to all their security products

Costs for fixing security vulnerabilities

- ✓ Adopt security practices early.
- ✓ Practiced everyday and throughout SDLC.

Developer First Security – Shift Left



Dependency Scanning and Dependabot: automatic CVE identification & remediation

GHAS

Secret Scanning: locate and invalidate exposed tokens.

- **Push Protection**: prevent unauthorized changes

GHAS

CodeQL for Code Scanning: find & warn about risky patterns in code

GitHub Advanced Security

Dependency scanning

Know your dependencies

Secret scanning

Find API tokens or other secrets exposed anywhere in your git history or issues / pull requests

Code scanning

Static analysis of every git push, integrated into the developer workflow and powered by CodeQL

Xebia | Xpirit

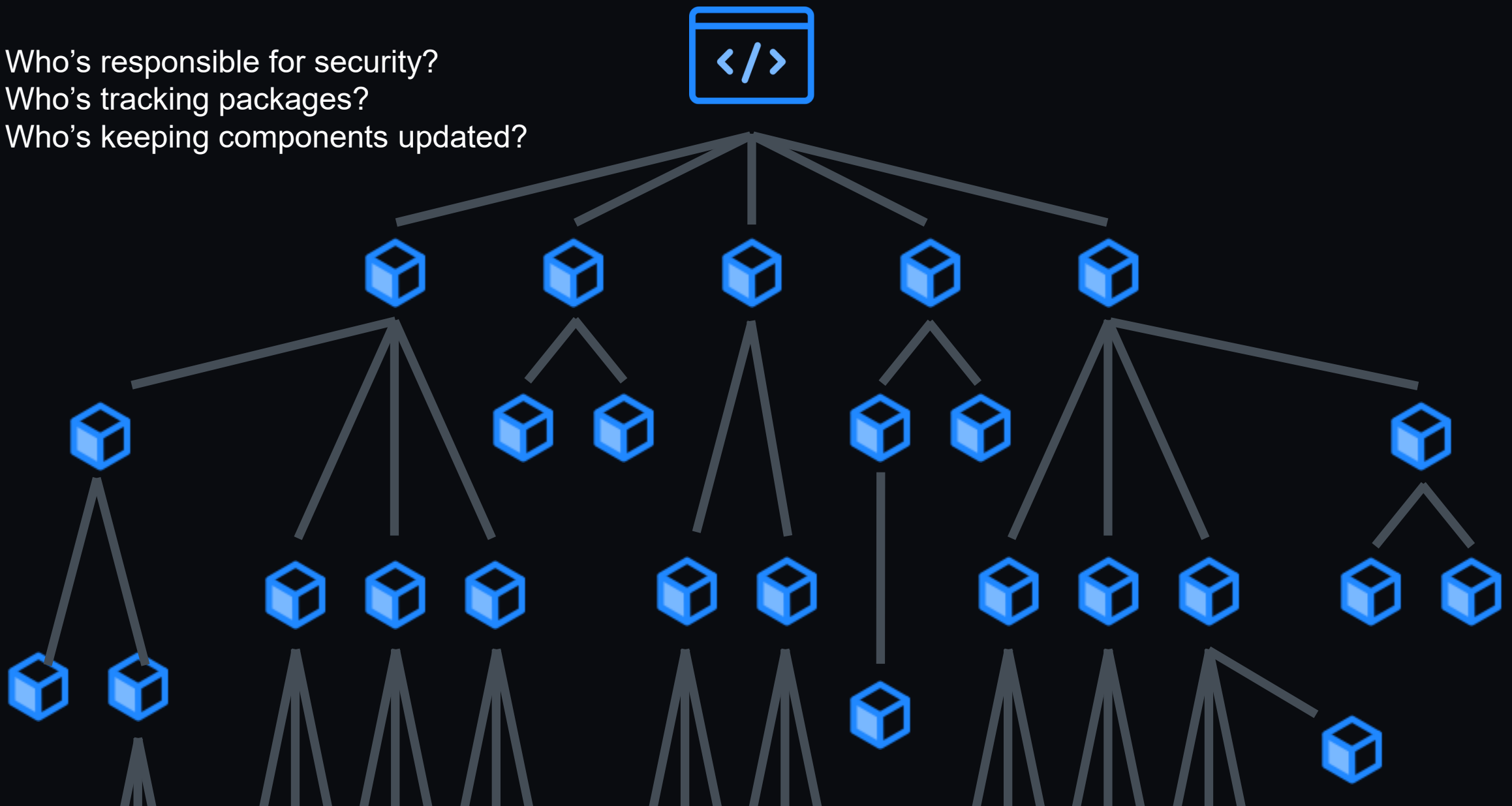
Licensing

- **GitHub**: Public Repos are Free
- **ADO**: Additional license - $49 / contributor / month
  - Contributor = active committer in the last 90 days
  - Deduplicated on the Organization level
  - Metered billing through your Azure Subscription
  - Pro-rated on a daily basis

Xebia | Xpirit

Securing your Supply Chain

Who’s responsible for security?
Who’s tracking packages?
Who’s keeping components updated?



Dependency Scanning Demo

GitHub Advanced Security

Dependency scanning

Know your dependencies

Secret scanning

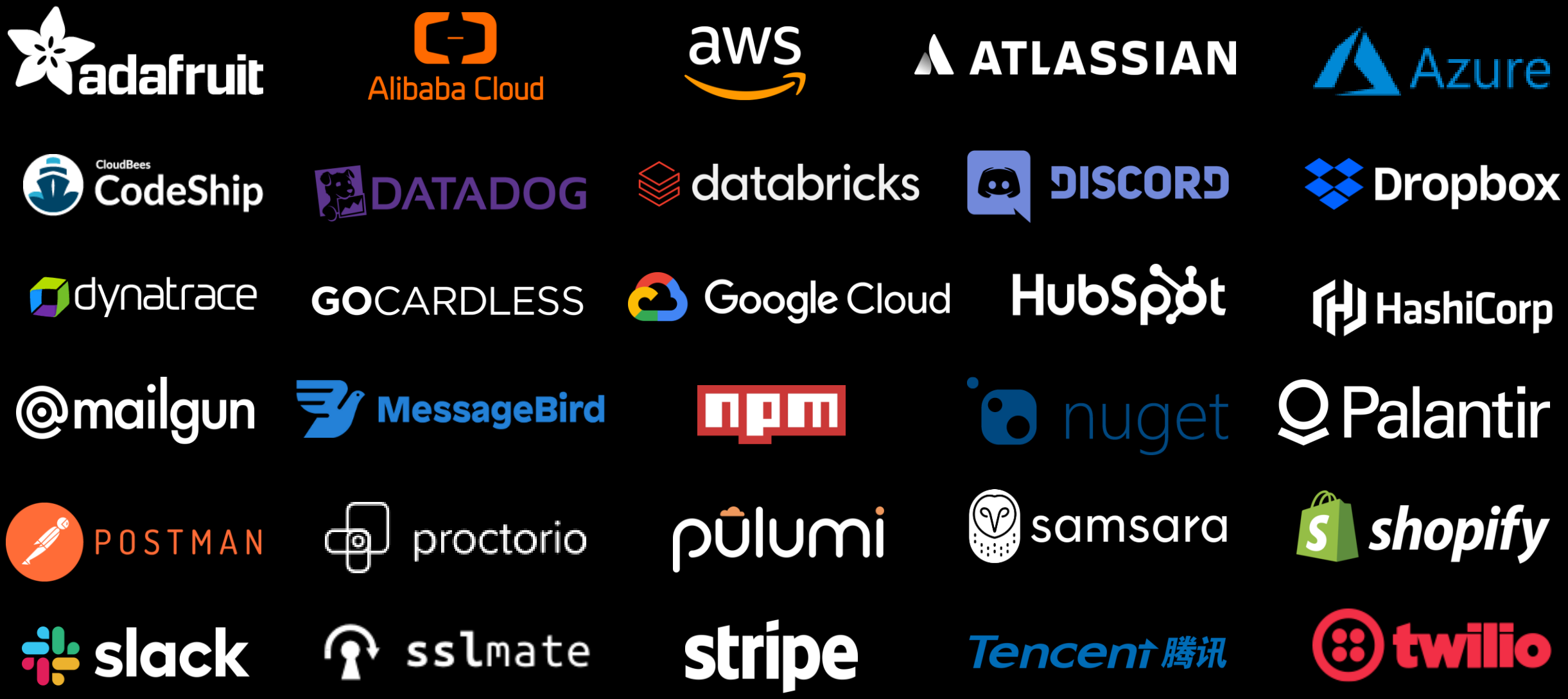
Find API tokens or other secrets exposed anywhere in your git history or issues / pull requests

Code scanning

Static analysis of every git push, integrated into the developer workflow and powered by CodeQL

Xebia | Xpirit

Secret Scanning Partners (60+)



Secret Scanning Demo

GitHub Advanced Security

Dependency scanning

Know your dependencies

Secret scanning

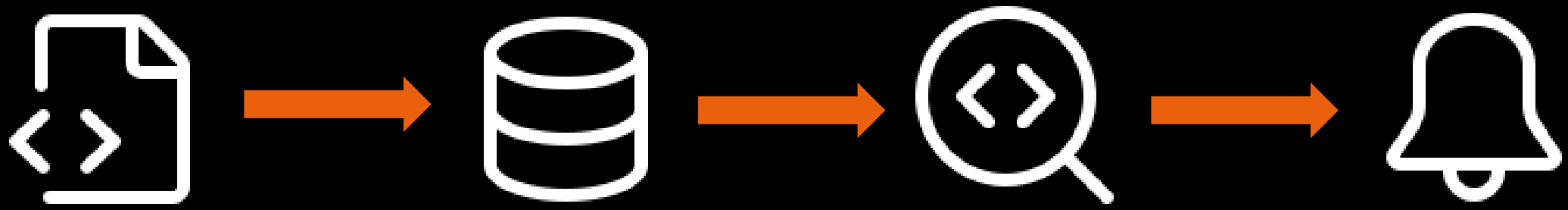
Find API tokens or other secrets exposed anywhere in your git history or issues / pull requests

Code scanning

Static analysis of every git push, integrated into the developer workflow and powered by CodeQL

Xebia | Xpirit

What is code scanning with CodeQL?



Combining CodeQL with the world's largest developer community gives next generation SAST performance

1,700+

open source queries
with contributions from Microsoft, Google and many others

72%

fix rate for potential vulnerabilities flagged in open source projects

15%

fix rate after 7 days

45%

fix rate after 90 days

24%

of recent JS CVEs would have been identified by a default CodeQL query

Code Scanning Demo

Similarities to GHAS

- Both have Secret Scanning & Push Protection
- Same list of supported security partners
- Both have CodeQL
- Both are tightly integrated in respective platforms
- ADO bills at $49/month per active committer
- GHAS free for public repos

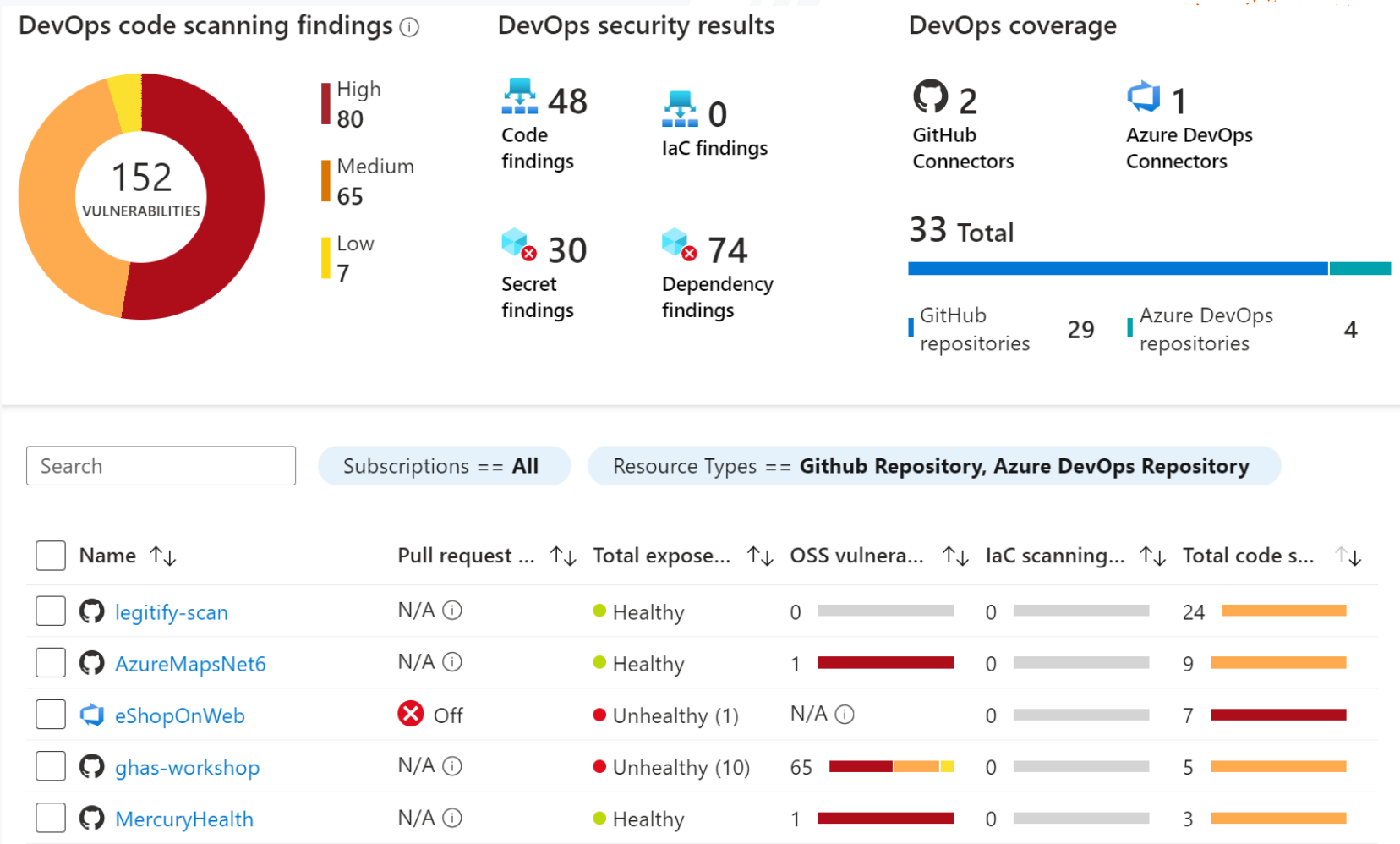
Differences to GHAS

- GHAS is always first
- Missing functionality on GHAzDo:
  - Numbers on alerts
  - PR blocking / Annotations not there yet
  - Dependabot PR’s (on roadmap no ETA)
  - No Security Overview. (Use DevOps extension by Rob Bos)
  - No pipeline failure on errors
- GitHub is more engineer centered (alerts)
- Custom secret scanning pattern
- Dependency graph visualization
- Custom CodeQL queries (ETA is early CY2024)
- GHAzDo pushes overview to Defender for DevOps

Microsoft Defender for Cloud

DevOps Security - Insights across multi-pipeline environments to prioritize remediation and apply security guardrails

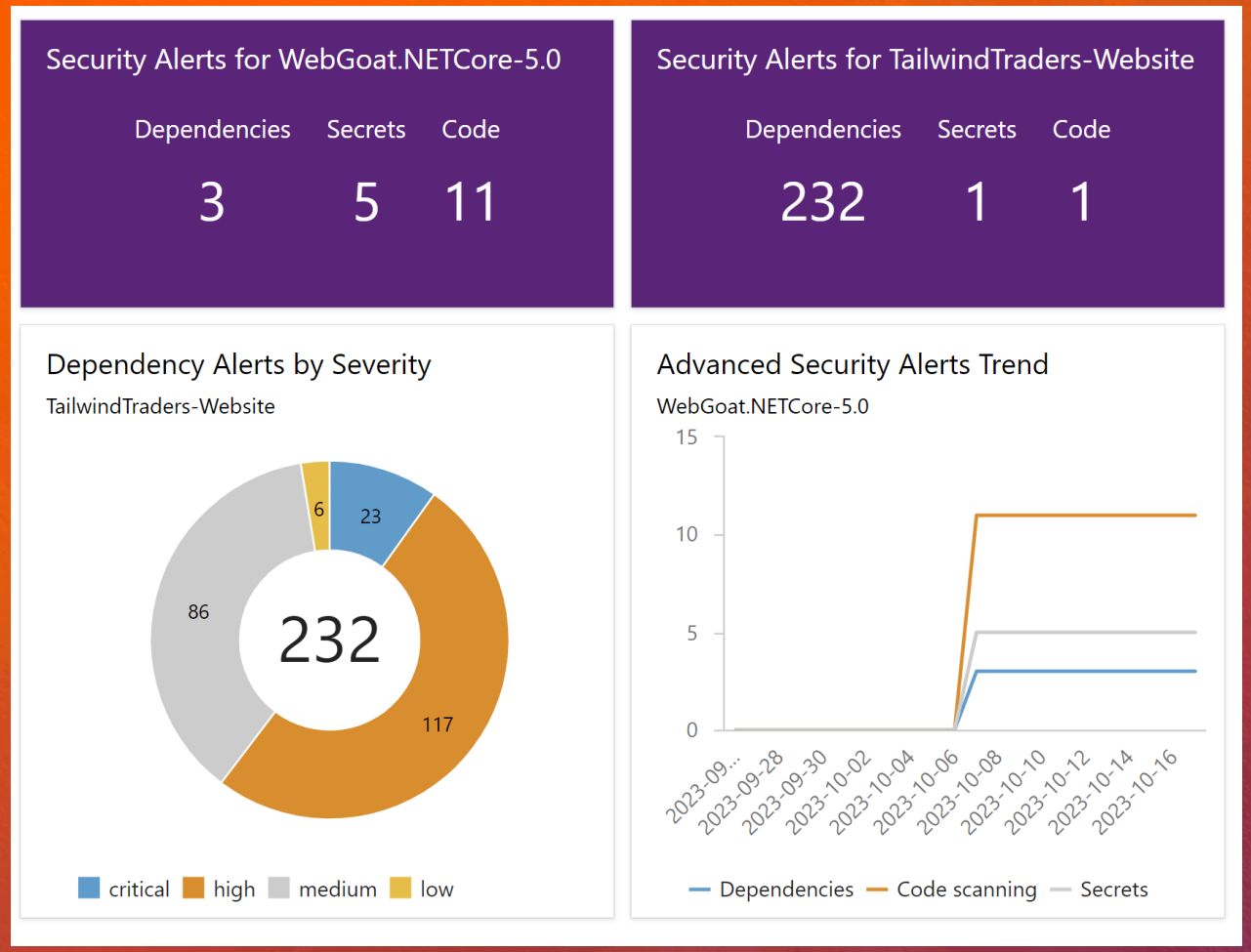
- Strengthen configuration of cloud resources throughout SDLC
- Provide unified, end-to-end visibility across departments
- Prioritize remediation of critical code issues using actionable feedback



Xebia | Xpirit

Advanced Security dashboard Widgets

Marketplace: https://marketplace.visualstudio.com/items?itemName=RobBos.GHAzDoWidget
Repo: https://github.com/rajbos/ghazDo-widget/



Xebia | Xpirit

Xebia | Xpirit

OpenAI Innovation

OpenAI Innovation

GitHub Copilot

Your AI pair programmer

- AI powered, context aware, code suggestions
- Understands dozens of languages
- Adapts to the edits you make, matching your coding style

77%

Spend less time searching

74%

Focus on more satisfying work

88%

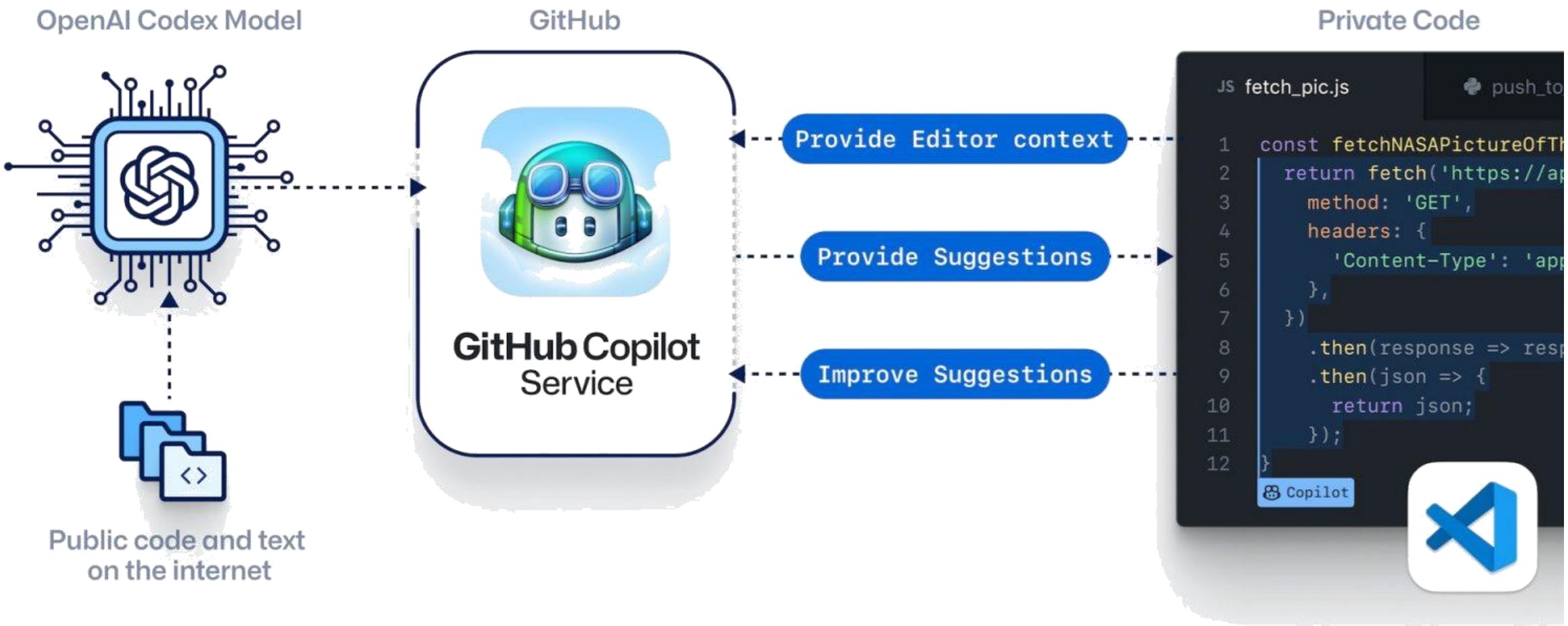
Feel more productive

72%

Are faster with repetitive tasks

https://github.com/Azure-Samples/azure-search-openai-demo

Copilot Architecture



Resources

Slide Deck: https://github.com/PagelsR/Talks

Webinar on Nov 2nd at 11am EDT

- 30-minute webinar recording: Embed security checks in your Azure DevOps Pipelines
- **https://lnkd.in/erF--7jZ**

Secure at every step

- https://resources.github.com/learn/pathways/security

GHAzDO

- **Blog:** https://devopsjournal.io/blog/2023/05/23/GitHub-Advanced-Security-Azure-DevOps
- **Bootcamp:** https://xpirit.com/github-advanced-security-for-azure-devops/

GHAS dashboard widgets for GHAzDO

- https://marketplace.visualstudio.com/items?itemName=RobBos.GHAzDoWidget

GitHub Advisory Database

- https://github.com/advisories

Code Scanning

- https://codeql.github.com/

Xebia | Xpirit


GHAzDO Bootcamp
Sign up for GitHub Advanced Security for Azure DevOps Today!!!
https://xpirit.com/github-advanced-security-for-azure-devops/
Xebia | Xpirit

Slides: https://github.com/PagelsR/Talks

Thank you!

https://xpir.it/ghazdo

https://www.linkedin.com/in/randy-pagels/

Xebia | Xpirit