

Innersource with GitHub

Enabling open source culture and best practices inside your organization

Increased collaboration

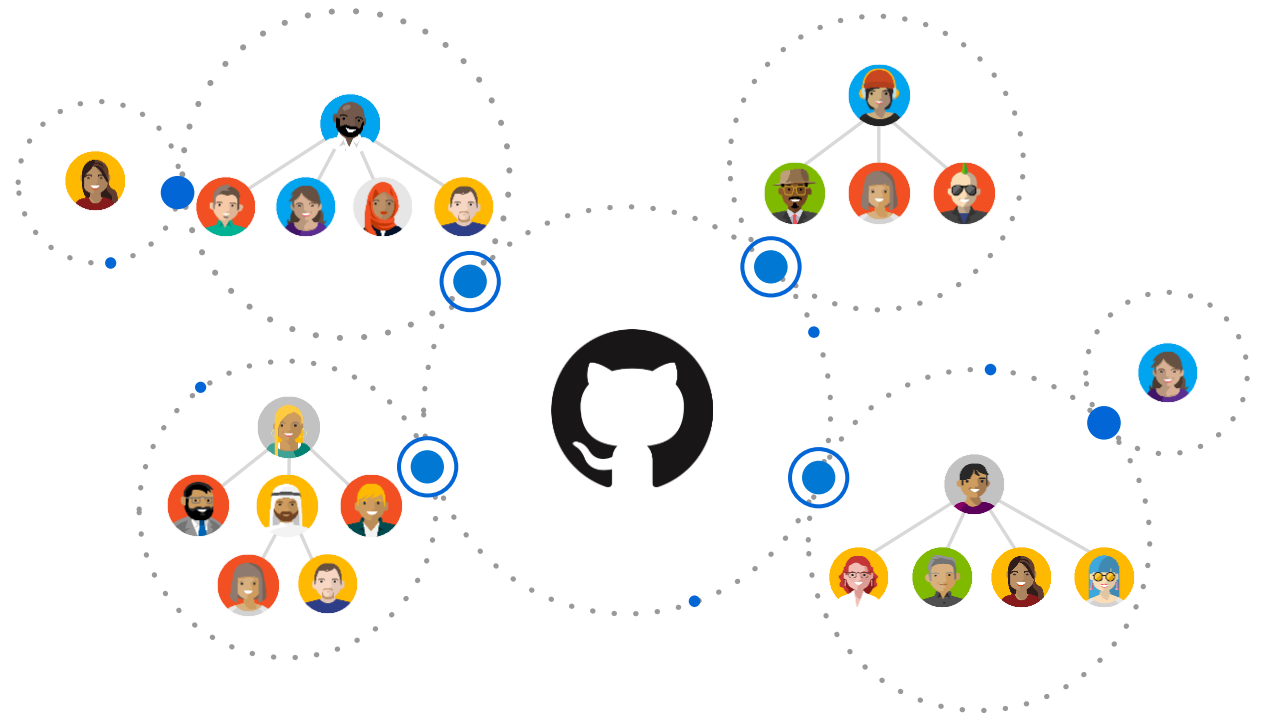
Encourage teams to collaborate within your organization using the same processes and practices as open source communities

Breaking silos

Simplified collaboration across teams, sharing of knowledge, improved code reuse, and secured workflows

Higher developer satisfaction

Leveraging inner source and open source practices increases developers' satisfaction, enabling them to work on interest projects and increase their skills



GitHub Advanced Security

Securing the software supply chain

Securing the usage of open source

Vulnerability Dependency Insights and automated security fixes with Dependabot.

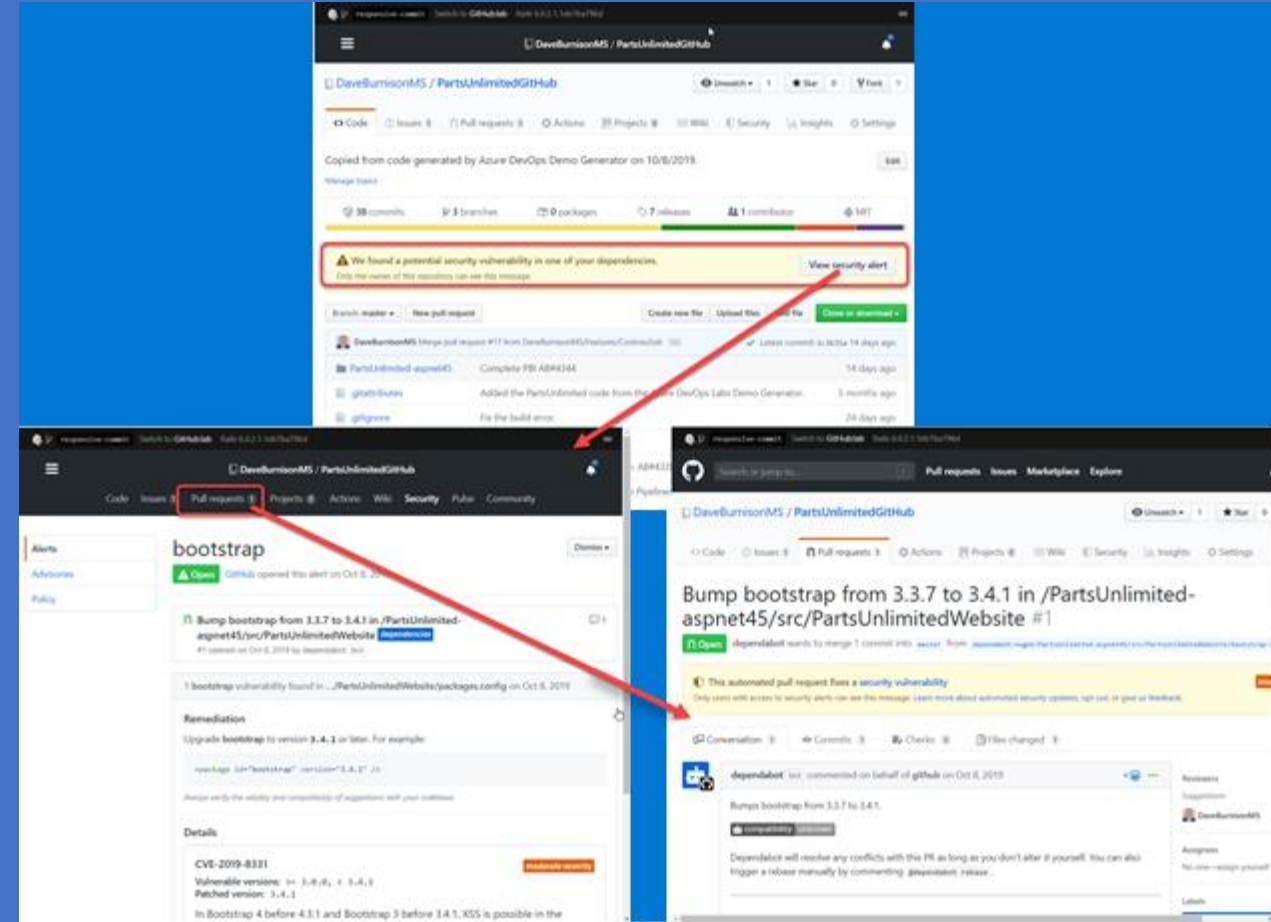
Pattern based security analysis

Always on security analysis with GitHub advanced security scanning both open source repositories and enterprise code.

Global community for security

Integrated into the National Vulnerability Database, MITRE, and WhiteSource for up-to-date security information.

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



Code Scanning

Preventing vulnerabilities from the start

Find and fix vulnerabilities fast

Find and fix vulnerabilities before they are merged into the code base with automated CodeQL scans.

Community of top security experts

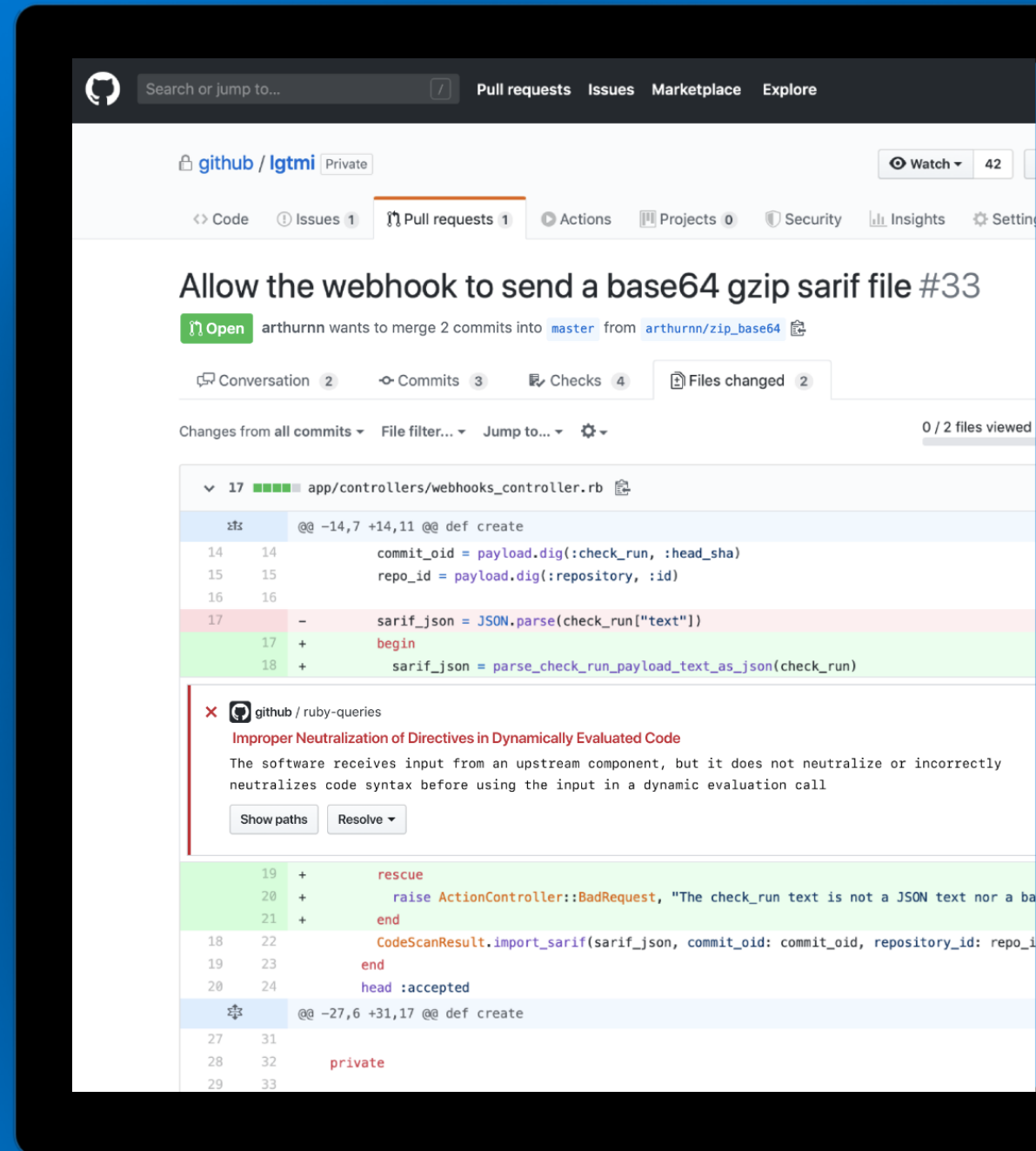
Community-driven query set powers every project with a world-class security team.

Integrated with developer workflow

Integrate security results directly into the developer workflow for a frictionless experience and faster development.

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

<https://github.blog/2020-09-30-code-scanning-is-now-available/>



Secret Scanning

Keeping your secrets, a secret

Identifies secrets as early as possible

Finds secrets the moment they are pushed to GitHub and immediately notifies developers when they are found.

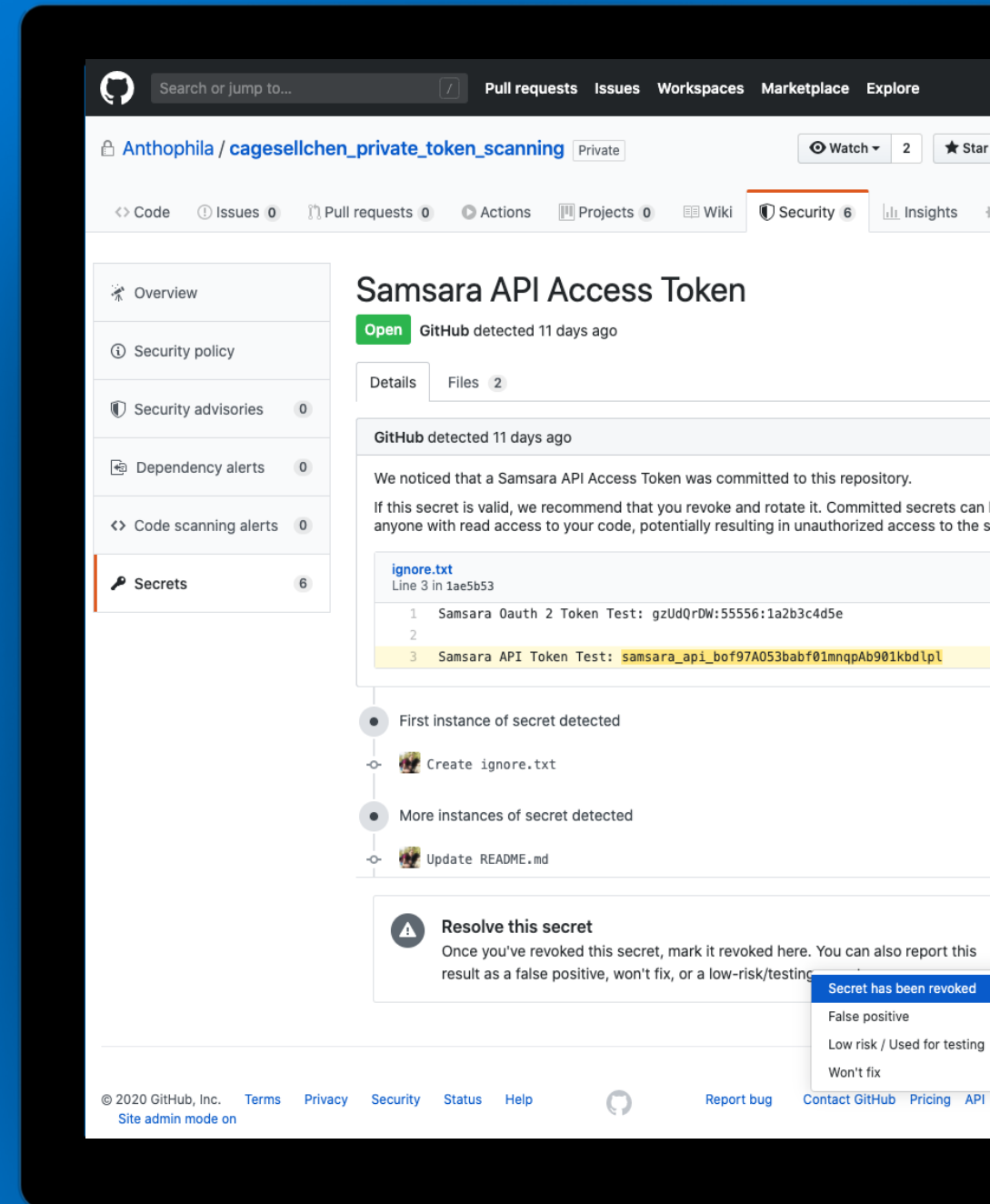
Community of secret scanning partners

For every commit made to your repository, and its full git history, we'll look for secret formats from secret scanning partners

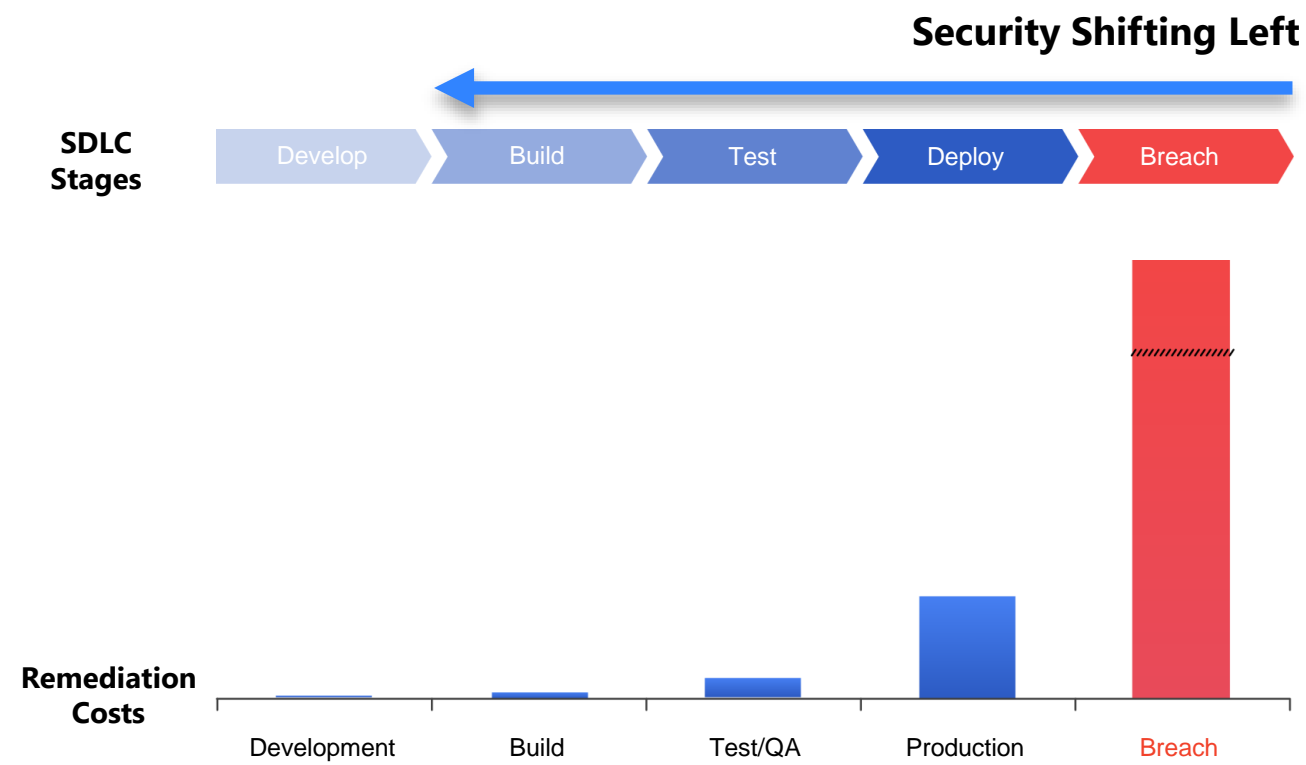
Supports both public and private repos

Secret scanning watches both public and private repos for potential secret vulnerabilities.

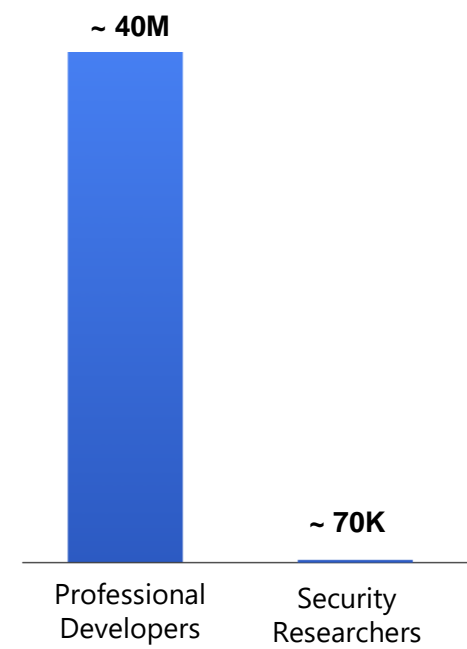
<https://github.com/features/security>



Shift security left with GitHub Advanced Security



Vastly more cost effective to remediate during development



570x more developers than security researchers



Codespaces

Your instant dev environment

Code without compromise

Code, build, test, debug, and deploy with a complete development environment in your browser.

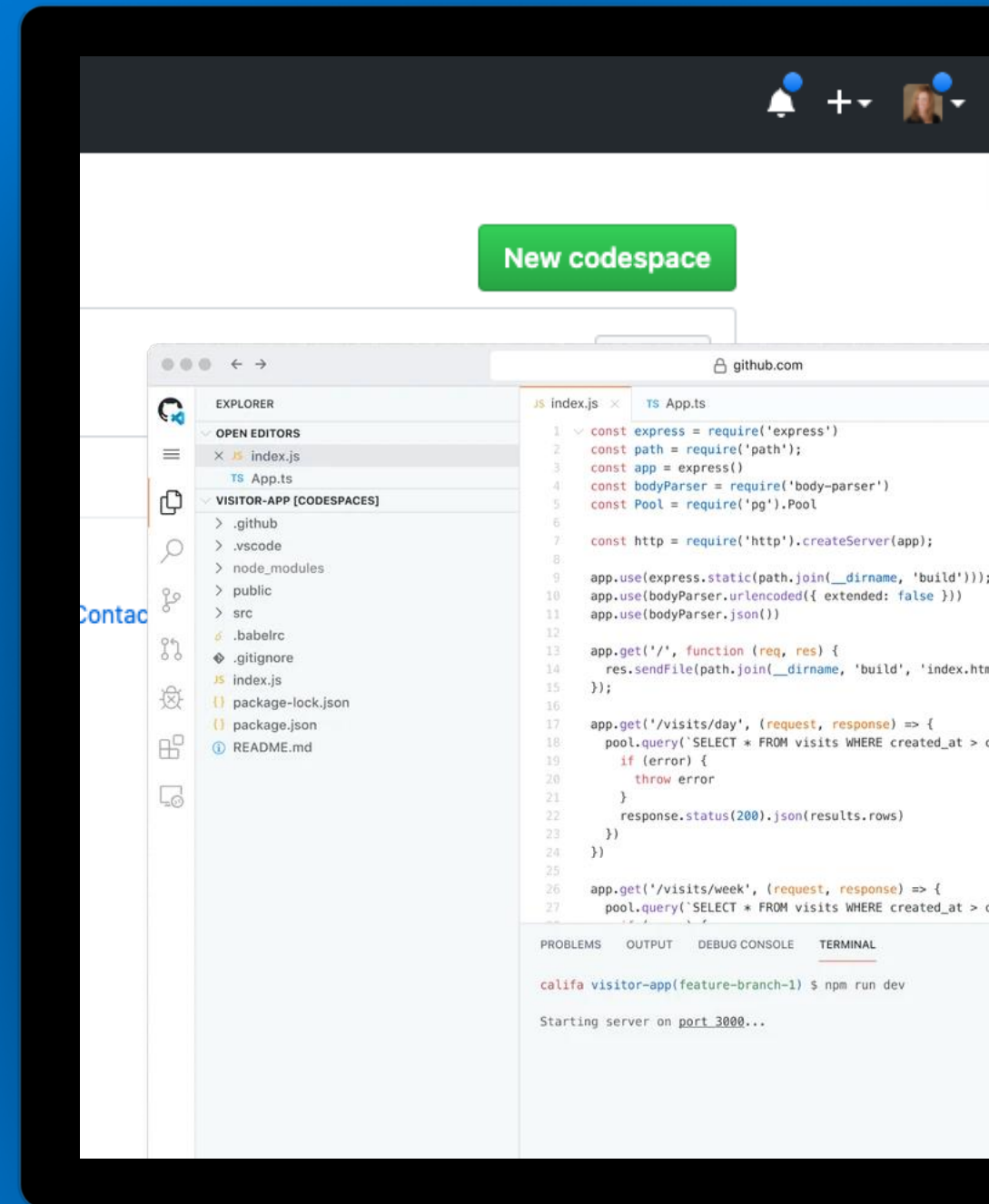
Simplify your workflow

Automatically set up dependencies and SSH keys.
Go from code to commit faster on any project.

Extend and customize

Configure your editor with dotfiles and VS Code extensions to create a consistent environment in every codespace.

<https://github.com/Features/Codespaces>



Automated Delivery

Automating workflows from code to cloud

Accelerate delivery through automation

Automation triggers for 20+ project events allows for automation beyond just CI/CD to any available API

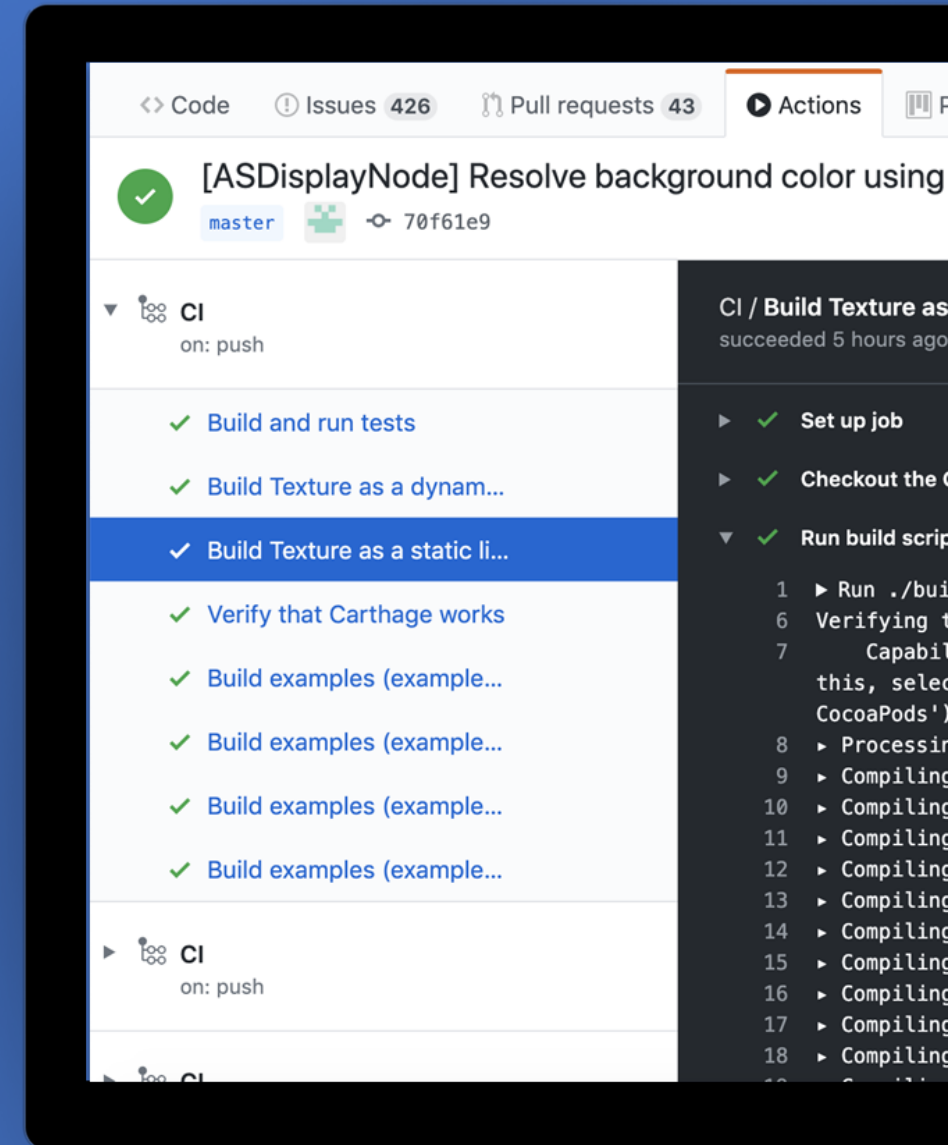
Simple and easy to use

Configuration based on YAML with a host of sample workflows to learn from and get started

Global community for actions

Thousands of open source Actions, maintained by the community and by companies offering integrations, including Microsoft Azure

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



GitHub Actions for Azure

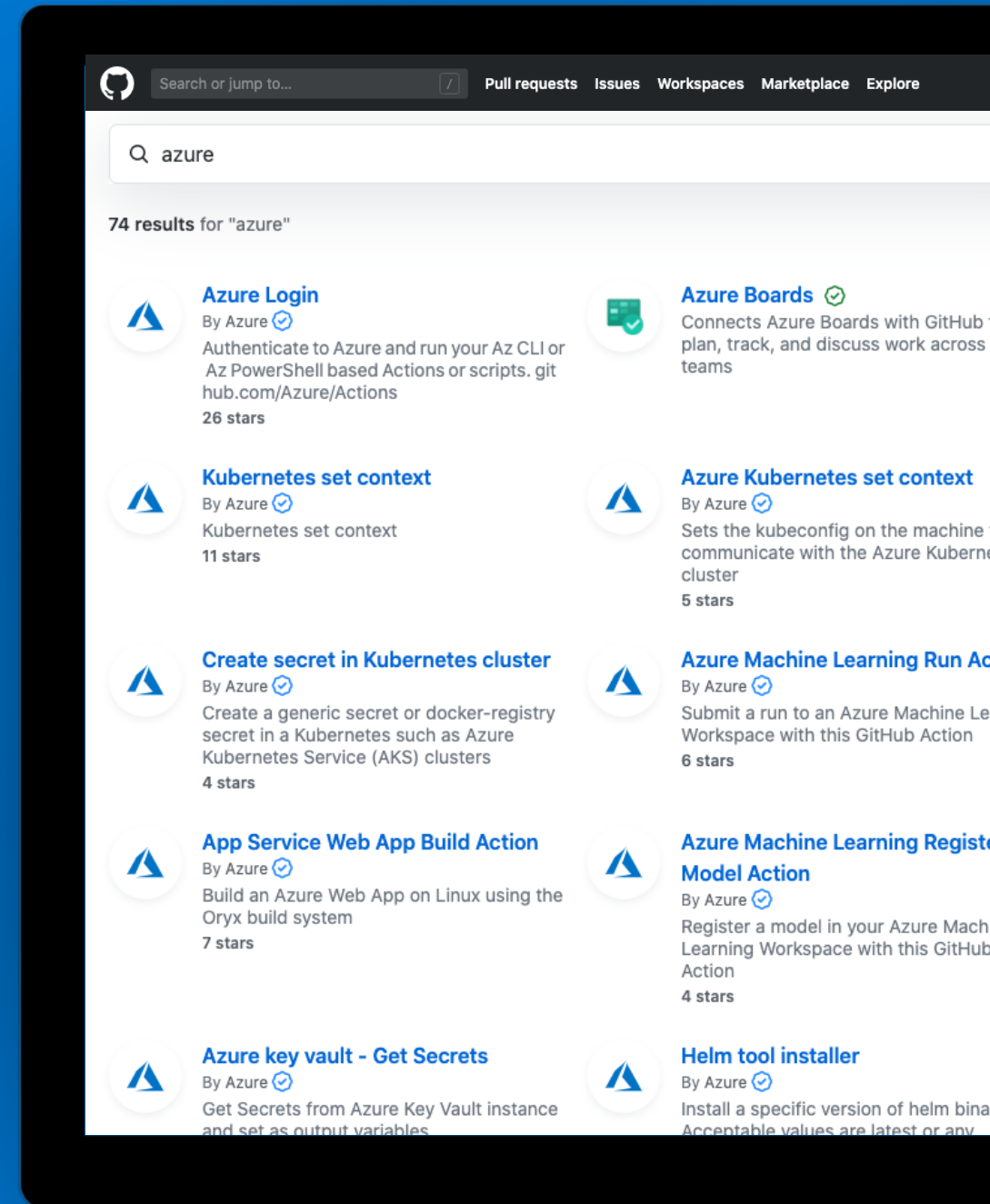
Over 70 ready-to-use actions for Azure

Deployment actions to Azure include:

- **Deploy to Kubernetes Cluster** – deploy a Kubernetes cluster, including AKS clusters
- **Azure WebApp** – deploy Web Apps or Containerized Web Apps to Azure.
- **Azure Functions Action** – deploy Function App to Azure Functions.
- **Azure SQL Deploy** – deploy a DACPAC or a SQL script to Azure SQL Database
- **Azure Machine Learning Deploy** – deploy a registered model in your Azure ML Workspace

Other popular Azure actions:

- **Azure CLI** – automate your workflow by executing Azure CLI commands to manage Azure resources inside of an Action
- **Azure Key Vault** – get secrets from Azure Key Vault instance and set as output variables.
- **Azure Policy Assignment with Azure CLI** - apply a policy to new infrastructure using Azure Policy (HIPAA, PCI-DSS, etc).
- **and many, many more...**



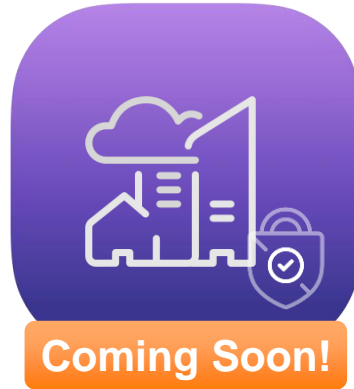
GitHub Enterprise Foundation



GitHub Enterprise Server

Self-managed & Flexible

Reliable and scalable solution packaged for self-managed deployments. Provides maximum flexibility and ease of operations.



Coming Soon!

GitHub AE (GHAE)

Secure & Fully Managed

For the most demanding deployments in regulated industries and government agencies. Cloud control plane, single tenant. FedRAMP certified.



GitHub Enterprise Cloud

Convenient & Reliable

Maximum convenience for fast growing enterprises. Multi-tenant, highly available service with 99.95% uptime.



What Does this Mean for the Future of Azure DevOps?

Microsoft is fully committed to Azure DevOps

We will continue to support and invest in Azure DevOps in the long term.

However, we are shifting our strategic investments to GitHub.

Going forward, our strategy is to bring the best of both products together into a single product experience in GitHub to provide the broadest set of software development capabilities that meet the needs of every enterprise.

Choose the Best Tool for each Phase - Today

DevOps Phase	Area	Azure DevOps	GitHub	Current Recommendation / Comments
Plan	Plan & Track	Boards	Issues & Projects	This is an area where we are aggressively working to build out features in GitHub. Key Gaps: Hierarchical Relationships, Plan in Sprints, Saved Issue Queries. Sprint Planning: Azure Boards integrated with GitHub. Basic Planning: GitHub Issues & Projects.
	Group think		Discussions	Organize conversations into a threaded format. Only available in GitHub.
Collaborate	SCM	Repos	Repos	Use GitHub to get value today from Advanced Security features, Innersource, developer familiarity w/ GitHub.
Develop	Advanced Coding		Codespaces	Integrated directly into and hosted by GitHub. Powered by Visual Studio Code. Only available in GitHub (In Beta as of January, 2021)
	Security Scanning	3rd Party Extensions	Advanced Security	Available natively in GitHub. Azure DevOps needs 3rd party extensions. This is an area of key differentiation between GitHub and other products. This shifts security to the left!
Deliver	Packages	Artifacts	Packages	GitHub Packages if you are using GitHub Repos. Otherwise, use Azure Artifacts
	CI/CD	Pipelines	Actions	This is an area where we are aggressively working to build out features in GitHub. Key gaps today: Centrally managed workflow templates, Report test-pass rate per workflow run. Use GitHub Actions if it fits your needs. Otherwise, use Azure Pipelines w/ integration to GitHub.
	Workflow Automation		Actions	GitHub Actions can be used for a lot more than just CI/CD. e.g. Send an email when a repo is cloned. You may have use cases today where you can use <u>both</u> Azure Pipelines and GitHub Actions.
	Manual Testing	Test Plans	N/A Today	Azure Test Plans as the GitHub solution is TBD (it is lower on the current priority list).
Operate, Monitor & Learn	Dashboards & Reporting	Dashboards & Reporting	Insights	Use Azure DevOps for now. Keep an eye on the roadmap for GitHub Insights. You may use both as there is valuable information in GitHub insights but, no configurable widgets yet.
All	Mobile Access		Mobile App	First class mobile experience for iOS and Android (no Windows Phone support). Only available for GitHub.

GitHub Actions & features

- Continuous integration and continuous delivery (CI/CD) platform that automates build, test, and deployment pipeline.
- Create workflows that build and test every pull request to your repository or deploy merged pull requests to production.



Live logs



Secret store

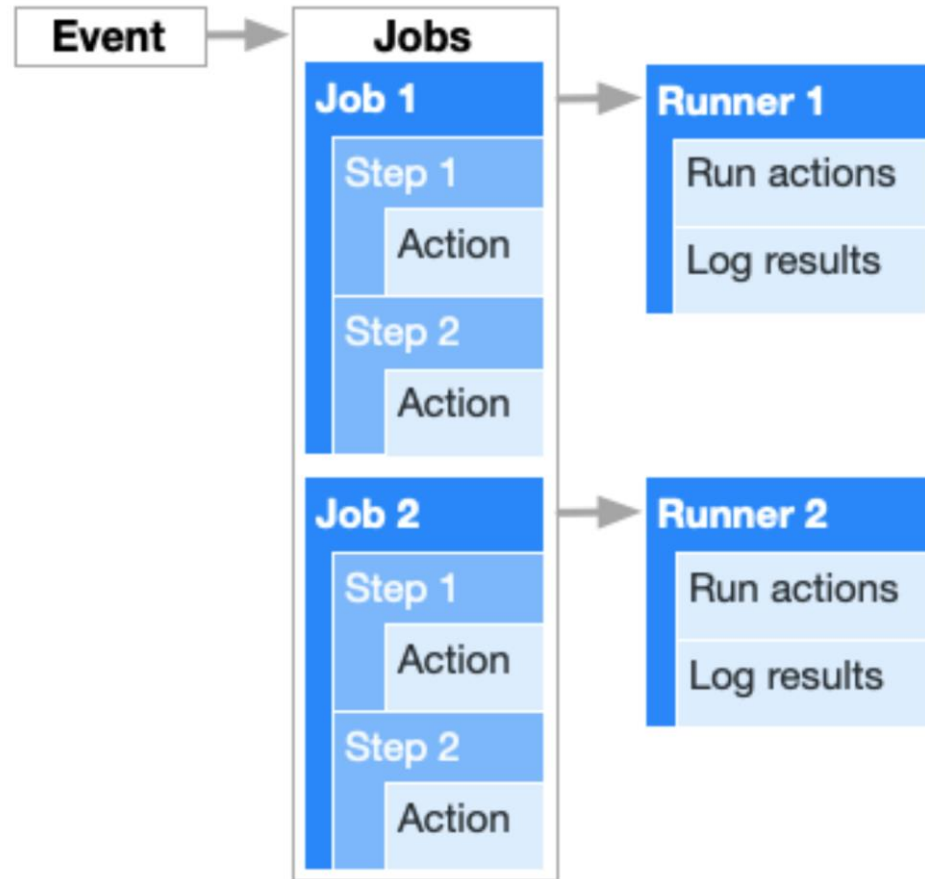


**Linux, macOS,
Windows, ARM,
and containers**



Matrix builds

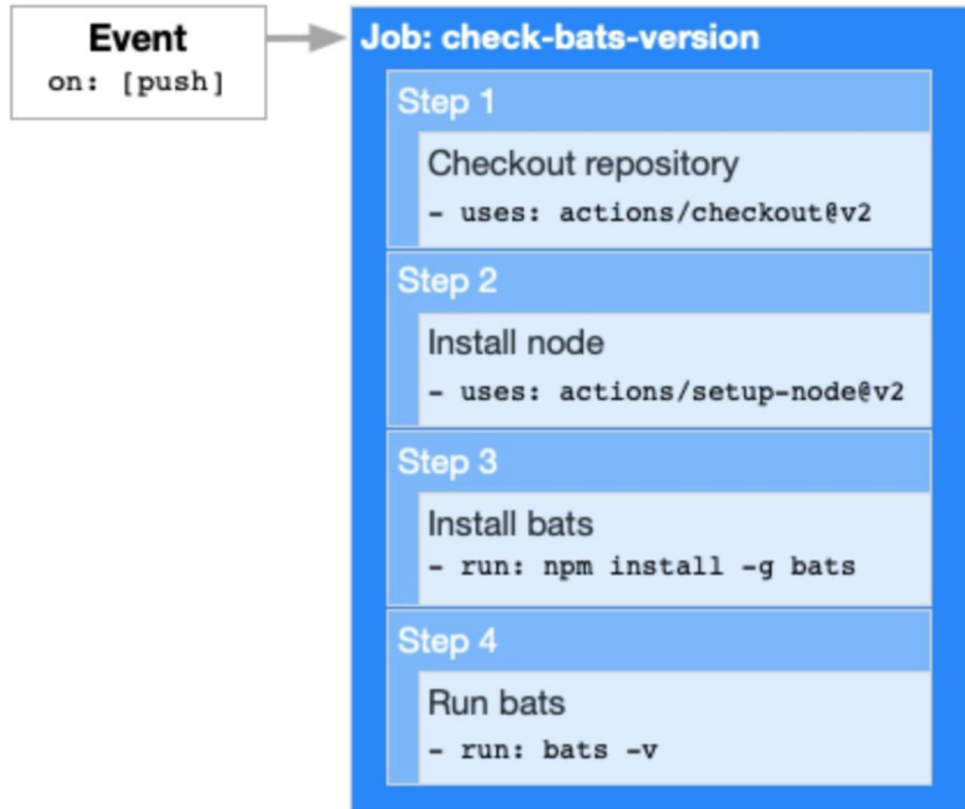
Components of a workflow



Each job will run inside its own virtual machine *runner*, or inside a container

Visualizing the Yaml workflow

```
name: learn-github-actions
on: [push]
jobs:
  check-bats-version:
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v2
      - uses: actions/setup-node@v2
        with:
          node-version: '14'
      - run: npm install -g bats
      - run: bats -v
```



Codespaces

<https://www.telerik.com/blogs/introduction-github-codespaces>

GitHub Advanced Security

- Code scanning
- Secret scanning
- Dependency review
- Security review

Automatically checks for known vulnerabilities as soon as you push code to GitHub, you do not have to add steps to your pipeline to do this. AND, when it finds a known vulnerability, it automatically creates a Pull Request if it can find a resolution to the known vulnerability.

GHAS – Code scanning

[Code scanning alerts](#) / #1

Arbitrary file write during zip extraction ("Zip Slip")

Dismiss alert

Open

in `main` 5 days ago

`code/src/Attendee/Attendee.cs:12`

```
9      {
10          public void WriteToDirectory(ZipArchiveEntry entry, string destDirectory)
11          {
12              string destFileName = Path.Combine(destDirectory, entry.FullName);

Unsanitized archive entry, which may contain '..', is used in a file system operation.

CodeQL Show paths

13          entry.ExtractToFile(destFileName);
14      }
15
```

Tool	Rule ID	Query
CodeQL	cs/zipslip	View source

Extracting files from a malicious zip archive without validating that the destination file path is within the destination directory can cause files outside the destination directory to be overwritten, due to the possible presence of directory traversal elements (..) in archive paths.

Show more

Severity

High

Affected branches

main

Tags

security


Weaknesses


CWE-22

GHAS – Secret scanning

Secret scanning alerts / Alert


GitHub Personal Access Token #1

[Open](#) GitHub Advanced Security detected a secret 3 months ago · `ghp_e8t2IX8Fyn09jJhQ98...` 

 **This secret is compromised**
Anyone with read access can discover secrets committed to this repository, potentially resulting in unauthorized access to your services.

Suggested action: If this secret is valid, rotate and then revoke it to avoid any unauthorized access.

Secret detected in 1 file

▼ `code/src/AttendeeSite/appsettings.json` 

```
9     "AllowedHosts": "*",
10    "ConnectionString": "ghp_e8t2IX8Fyn09jJhQ98NJYAjiotBRaX1sQ50Z"
11  }
```

GHAS – Dependency graph

The screenshot shows the GitHub Security Dashboard interface. At the top, there are tabs for 'Insights' (selected) and 'Settings'. On the left sidebar, there are navigation links: Pulse, Contributors, Community, Traffic, Commits, Code frequency, **Dependency graph** (highlighted), Network, and Forks. The main content area is titled 'Dependency graph' and has three sub-tabs: 'Dependencies' (selected), 'Dependents', and 'Dependabot'. A prominent warning message is displayed: 'We found a potential security vulnerability in one of your dependencies. A dependency defined in .../SFBBot-UCWA/packages.config has known security vulnerabilities and should be updated.' Below this message is a button labeled 'View Dependabot alerts' and a note stating 'Only the owner of this repository can see this message.' Further down, a text block explains that these dependencies are defined in 'gh-demo's manifest files, such as .../SFBBot-UCWA/packages.config, .../SFBBot-UCWA/SFBBot-UCWA.csproj, and .../Attendee/Attendee.csproj.' At the bottom, a summary bar shows 'Dependencies defined in .../SFBBot-UCWA/packages.config' with a badge indicating 19 dependencies.

Insights Settings

Pulse

Contributors

Community

Traffic

Commits

Code frequency


Dependency graph

Network

Forks

Dependency graph


Dependencies Dependents Dependabot

 We found a potential security vulnerability in one of your dependencies.
A dependency defined in .../SFBBot-UCWA/packages.config has known security vulnerabilities and should be updated.

[View Dependabot alerts](#)

Only the owner of this repository can see this message.

These dependencies are defined in gh-demo's manifest files, such as .../SFBBot-UCWA/packages.config, .../SFBBot-UCWA/SFBBot-UCWA.csproj, and .../Attendee/Attendee.csproj.

 Dependencies defined in .../SFBBot-UCWA/packages.config 19

GHAS – Security overview

Security Overview

Risk 719 repositories

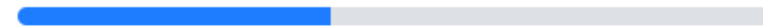
Distribution of risk across your organization



- High 371
- Medium 33
- Low 24
- Unknown 276
- Clear 15

Features enabled

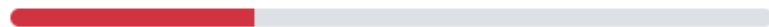
Distribution of all features enabled across your organization



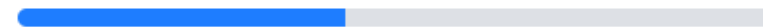
- All enabled 299/719

[Show less ^](#)

Code scanning 39,675 alerts



- Repositories with alerts 237



- Repositories enabled 313/719

Dependabot 2,006 alerts

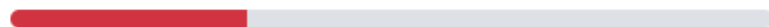


- Critical 63
- High 877
- Moderate 438
- Low 628



- Repositories enabled 718/719

Secret scanning



- Repositories with secrets detected 224



- Repositories enabled 706/719