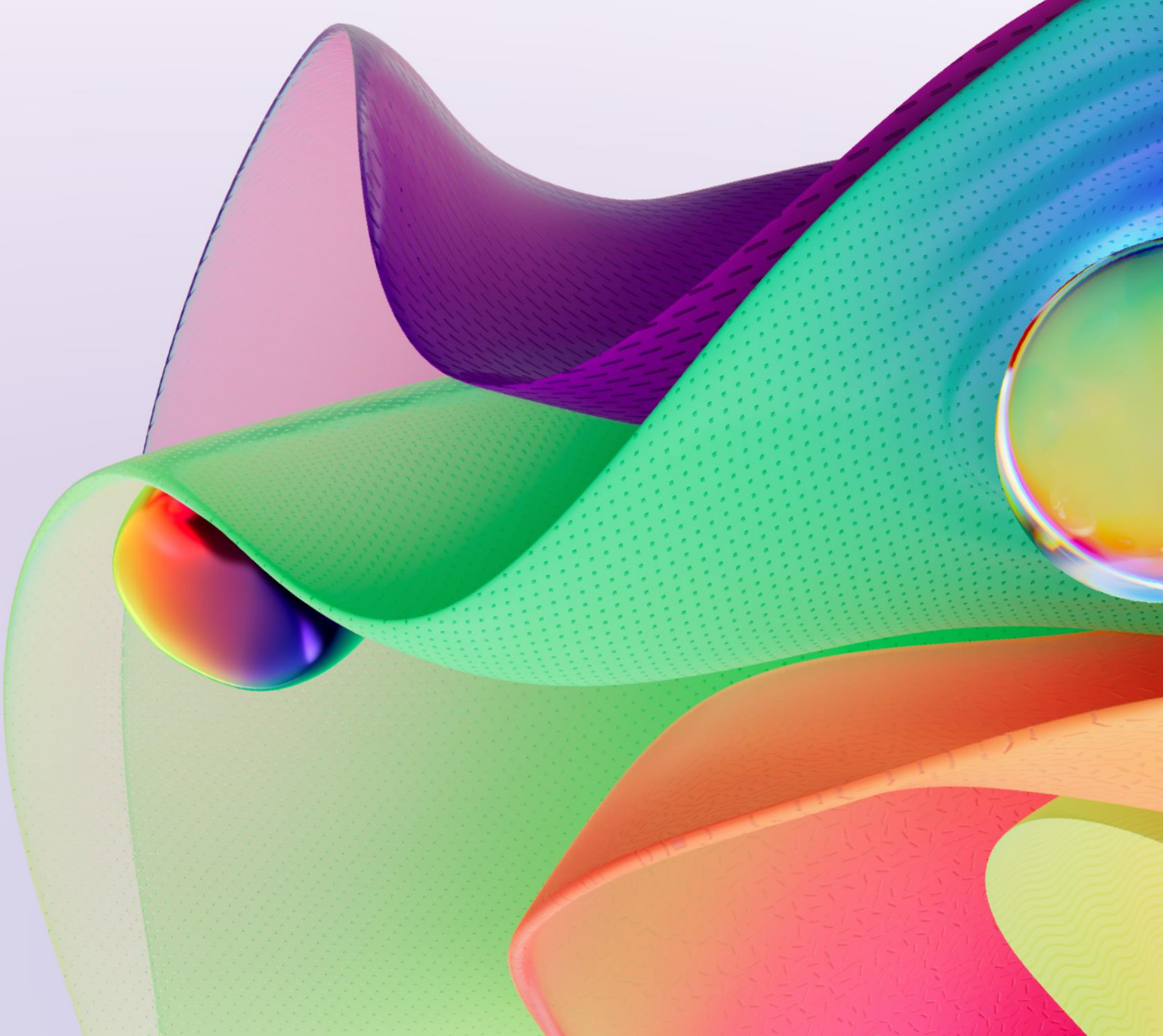
Microsoft

Microsoft AI Tour

In partnership with NVIDIA



Microsoft

Future of Security with AI

Joylynn Kirui
Senior Cloud Security Advocate
Microsoft

X: @joylynn_kirui

Agenda

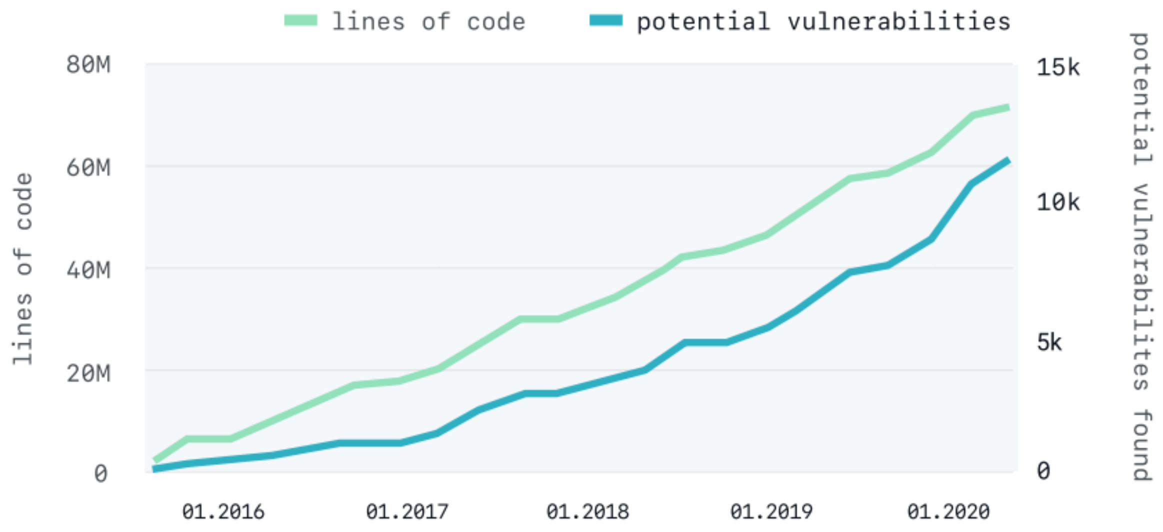
Introduction

Using GitHub Advanced Security to develop code securely

Using Security Copilot to democratize security for developers

The state of AppSec

Potential vulnerabilities found in source code scale with lines of code written



Despite billions of dollars of investment...

85% Of applications still contain a security issue.

Code written in 2020 is just as likely to introduce a security issue as code written in 2016.

Flaws in applications are consistently the #1 attack vector for breaches

The state of AppSec

Is falling further behind the current state of Development

1:100 Security team members to developers

Lack of knowledge voted the main AppSec challenge

Remediation trends are stagnant

Source: Verizon Data Breach Investigations reports 2016, 2017, 2018, 2019 and 2020.

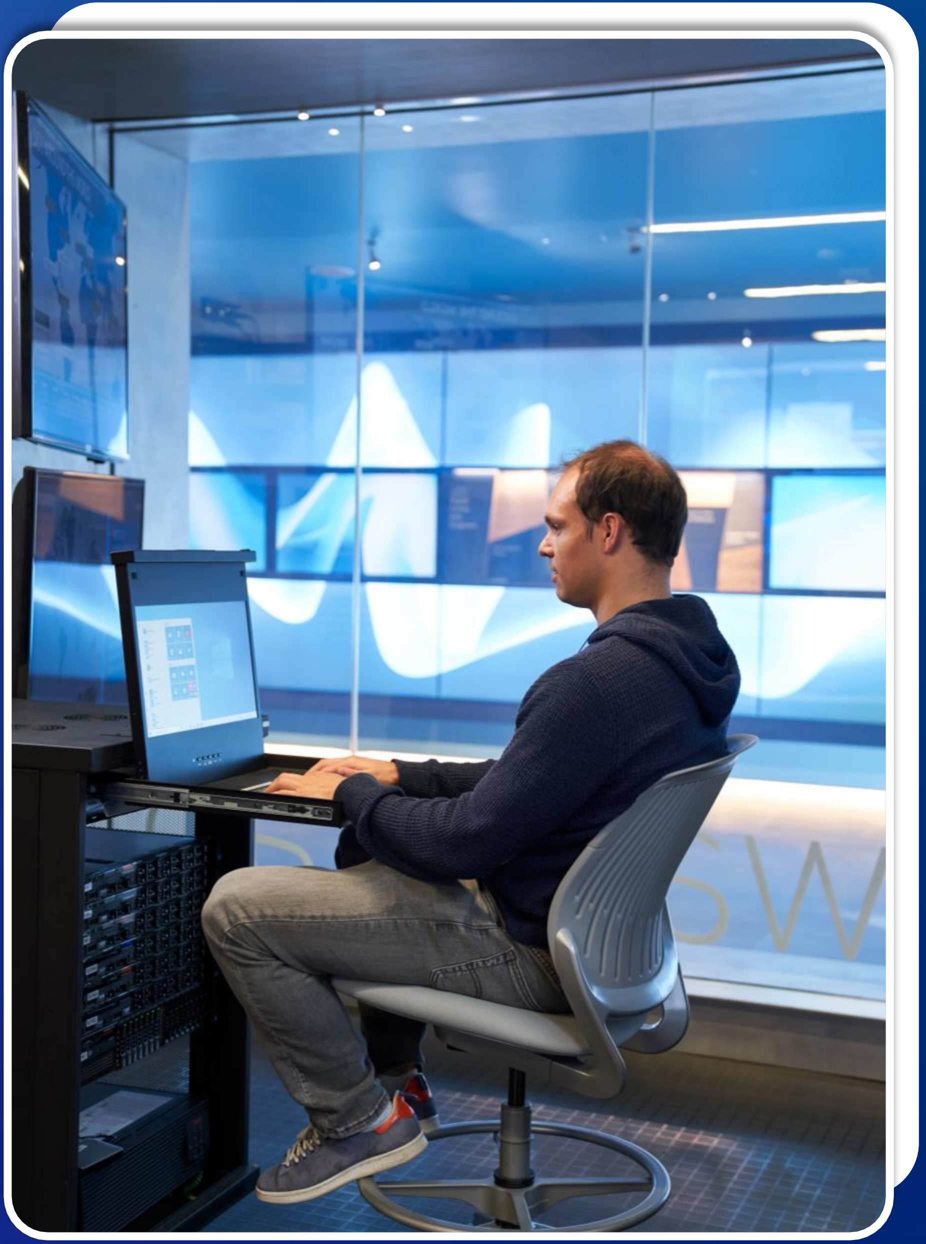
The odds are against today's security analysts

4,000 Password attacks per second

72 mins Median time for an attacker to access your private data if you fall victim to a phishing email

3.5M Global shortage of skilled cybersecurity professionals

Using GitHub Advanced Security to develop code securely



Current capabilities (core attributes)

Supply chain

Dependency graph
View your dependencies

Advisory database
Canonical database of dependency vulnerabilities

Security alerts and updates
Notifications for vulnerabilities in your dependencies, and pull requests to fix them

Dependency review
Identify new dependencies and vulnerabilities in a PR

Code

Secret scanning
Find API tokens or other secrets exposed anywhere in your git history

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

Development lifecycle

Branch protection
Enforce requirement for pushing to a branch or merging PRs

Commit signing
Enforce requirement that all commits are signed

Supply Chain

Dependabot

Automatically update vulnerable and out-of-date dependencies

Automated pull requests for security & version updates

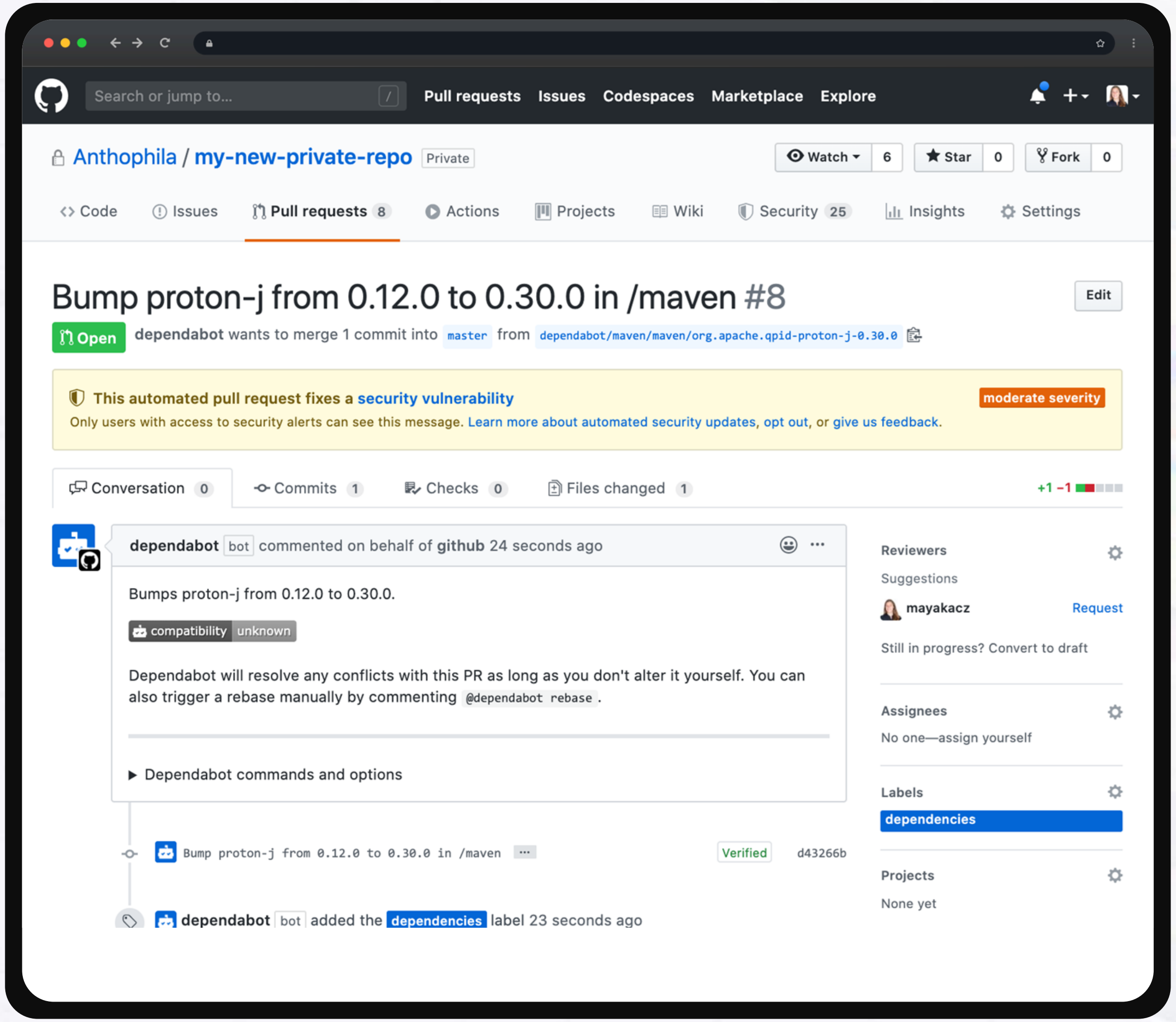
Keep your projects secure and up to date by monitoring them for vulnerable and out-of-date components. If a suggested update is found, we'll automatically open a pull request with suggested fixes.

Integrated with developer workflow

Dependabot is integrated directly into the developer workflow for a frictionless experience and faster fixes.

Rich vulnerability data

GitHub tracks vulnerabilities in packages from supported package managers using data from security researchers, maintainers, and the National Vulnerability Database—all discoverable in the GitHub Advisory Database.



Bump proton-j from 0.12.0 to 0.30.0 in /maven #8

Open dependabot wants to merge 1 commit into `master` from `dependabot/maven/maven/org.apache.qpid-proton-j-0.30.0`

This automated pull request fixes a security vulnerability moderate severity

Only users with access to security alerts can see this message. Learn more about automated security updates, opt out, or give us feedback.

dependabot bot commented on behalf of **github** 24 seconds ago

Bumps proton-j from 0.12.0 to 0.30.0.

compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

▶ Dependabot commands and options

`Bump proton-j from 0.12.0 to 0.30.0 in /maven` … Verified d43266b

dependabot bot added the dependencies label 23 seconds ago

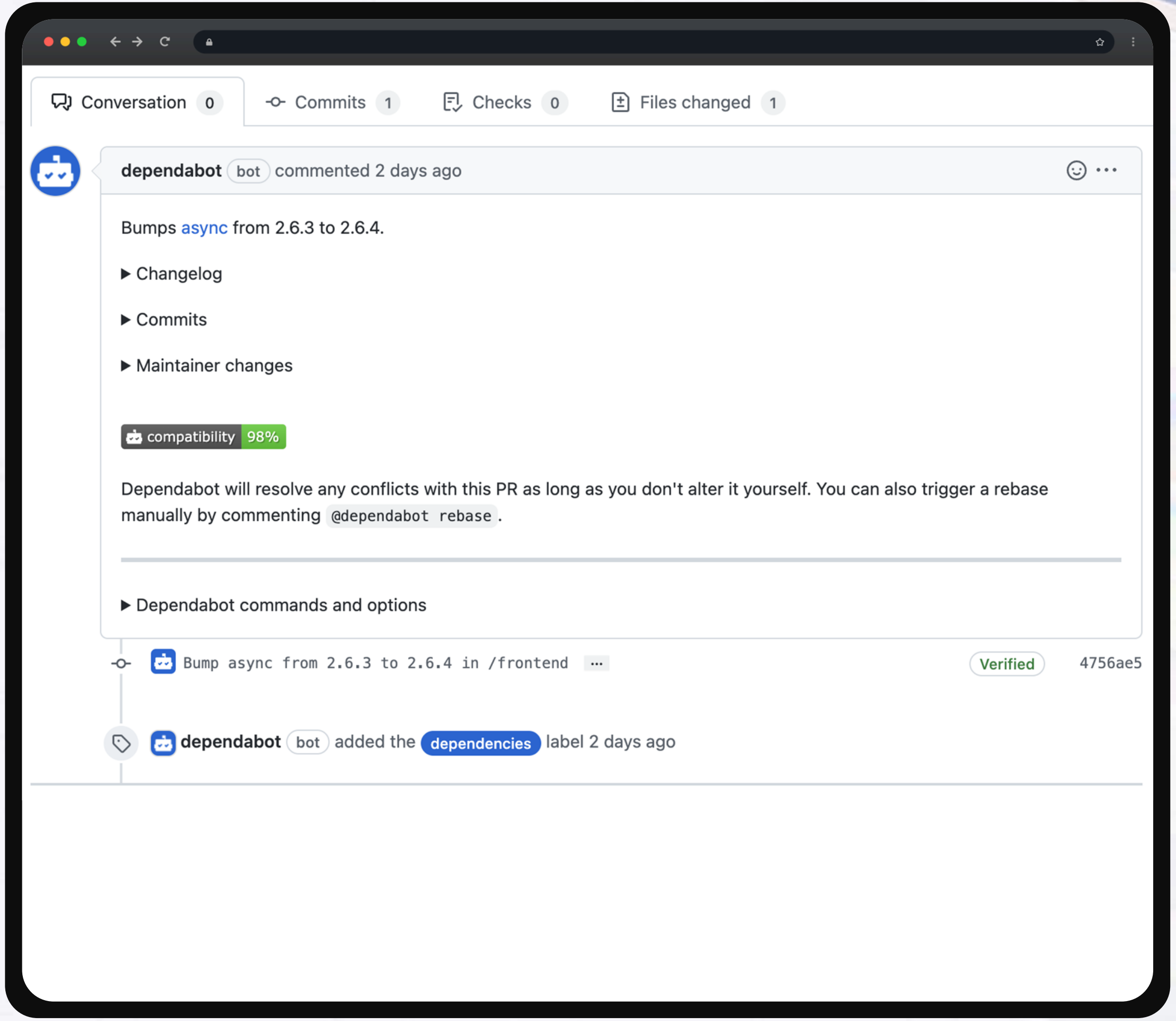
Dependabot

Automatically raise alerts when vulnerable dependencies are detected.

Automatically open pull requests to fix dependency vulnerabilities.

Notify the appropriate people about the vulnerability.

Rate the compatibility of a vulnerability patch.



dependabot bot commented 2 days ago

Bumps async from 2.6.3 to 2.6.4.

▶ Changelog

▶ Commits

▶ Maintainer changes

compatibility 98%

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

▶ Dependabot commands and options

```
Bump async from 2.6.3 to 2.6.4 in /frontend
```

Verified 4756ae5

dependabot bot added the dependencies label 2 days ago

Secret Scanning

Secret scanning

Find and manage hard-coded secrets

Identifies secrets as early as possible

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

Community of secret scanning partners

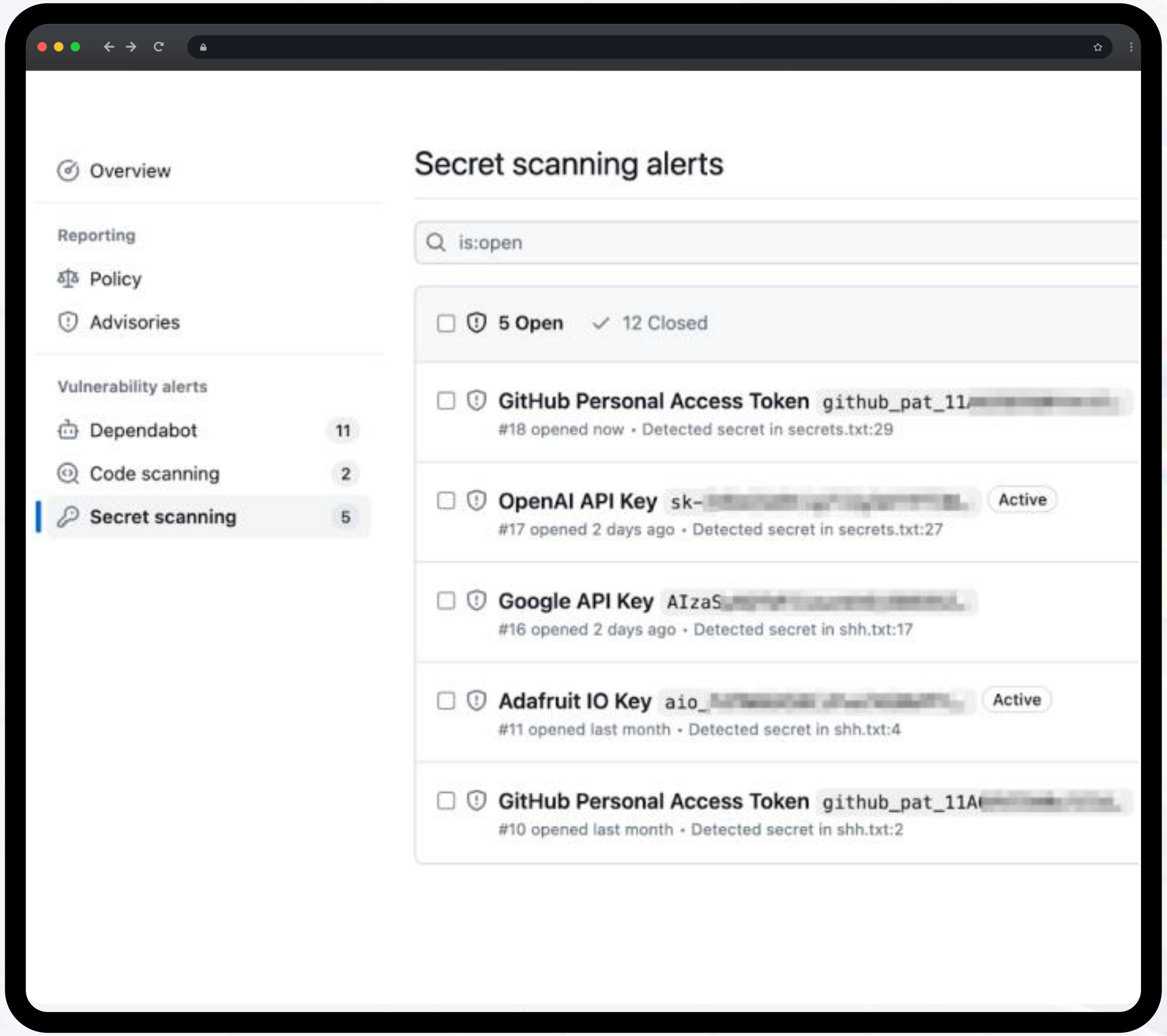
For every commit made to your repository and its full git history, we'll look for secret formats from secret scanning partners.

Define custom patterns

Scan for patterns that are internal to your organization across your repositories.

Supports both public and private repos

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



Overview

Reporting

Policy

Advisories

Vulnerability alerts

Dependabot 11

Code scanning 2

Secret scanning 5

Secret scanning alerts

is:open

□ 5 Open ✓ 12 Closed

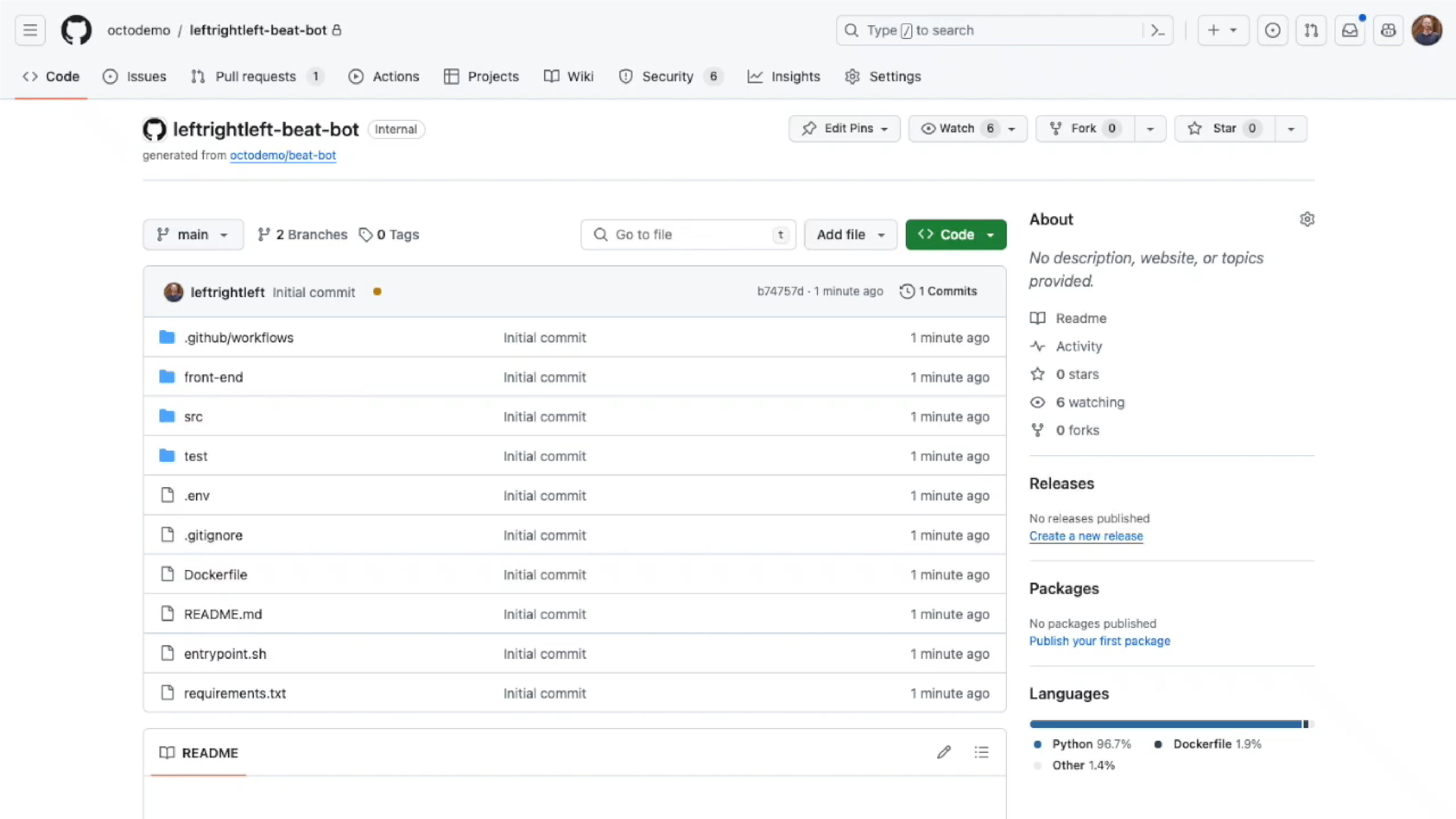
□ GitHub Personal Access Token `github_pat_11`[redacted]
#18 opened now • Detected secret in secrets.txt:29

□ OpenAI API Key `sk-`[redacted] Active
#17 opened 2 days ago • Detected secret in secrets.txt:27

□ Google API Key `AIzaS`[redacted]
#16 opened 2 days ago • Detected secret in shh.txt:17

□ Adafruit IO Key `aio_`[redacted] Active
#11 opened last month • Detected secret in shh.txt:4

□ GitHub Personal Access Token `github_pat_11A`[redacted]
#10 opened last month • Detected secret in shh.txt:2



leftrightleft-beat-bot

Internal

generated from octodemo/beat-bot

leftrightleft Initial commit · b74757d · 1 minute ago · 1 Commits

.github/workflows	Initial commit	1 minute ago
front-end	Initial commit	1 minute ago
src	Initial commit	1 minute ago
test	Initial commit	1 minute ago
.env	Initial commit	1 minute ago
.gitignore	Initial commit	1 minute ago
Dockerfile	Initial commit	1 minute ago
README.md	Initial commit	1 minute ago
entrypoint.sh	Initial commit	1 minute ago
requirements.txt	Initial commit	1 minute ago

About

No description, website, or topics provided.

- Readme
- Activity
- 0 stars
- 6 watching
- 0 forks

Releases

No releases published

Create a new release

Packages

No packages published

Publish your first package

Languages

● Python	96.7%
● Dockerfile	1.9%
● Other	1.4%

Code Scanning

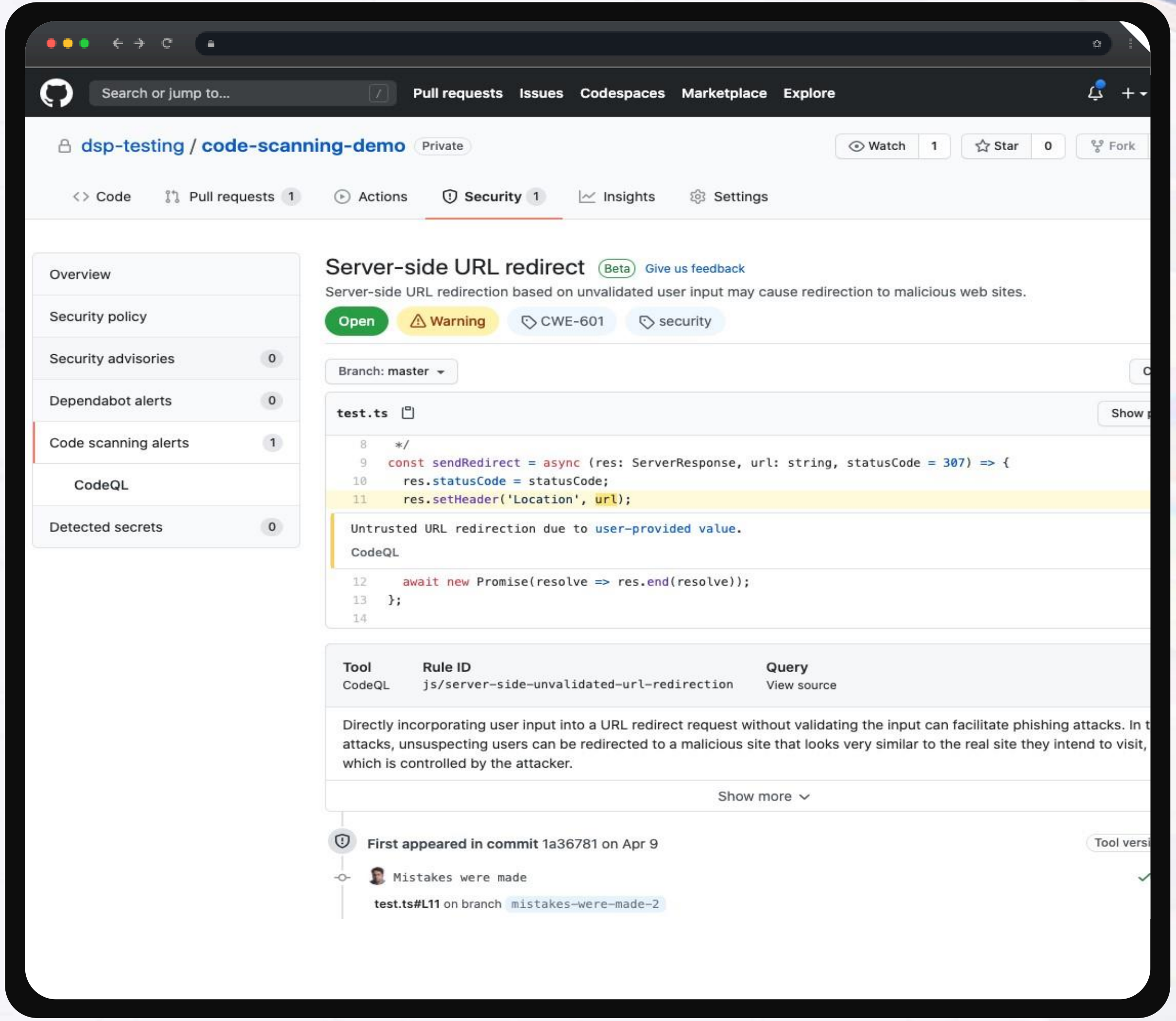
Code Scanning

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

Integrate results directly into the developer workflow.

Run custom queries and the community-powered GitHub query set.

Extensible, with support for other SAST tools.



Server-side URL redirect

Server-side URL redirection based on unvalidated user input may cause redirection to malicious web sites.

```
  */
const sendRedirect = async (res: ServerResponse, url: string, statusCode = 307) => {
  res.statusCode = statusCode;
  res.setHeader('Location', url);
```

Untrusted URL redirection due to user-provided value.

CodeQL

```
  await new Promise(resolve => res.end(resolve));
};
```

Tool	Rule ID	Query
CodeQL	js/server-side-unvalidated-url-redirection	View source

Directly incorporating user input into a URL redirect request without validating the input can facilitate phishing attacks. In t attacks, unsuspecting users can be redirected to a malicious site that looks very similar to the real site they intend to visit, which is controlled by the attacker.

First appeared in commit 1a36781 on Apr 9

Mistakes were made

test.ts#L11 on branch mistakes-were-made-2

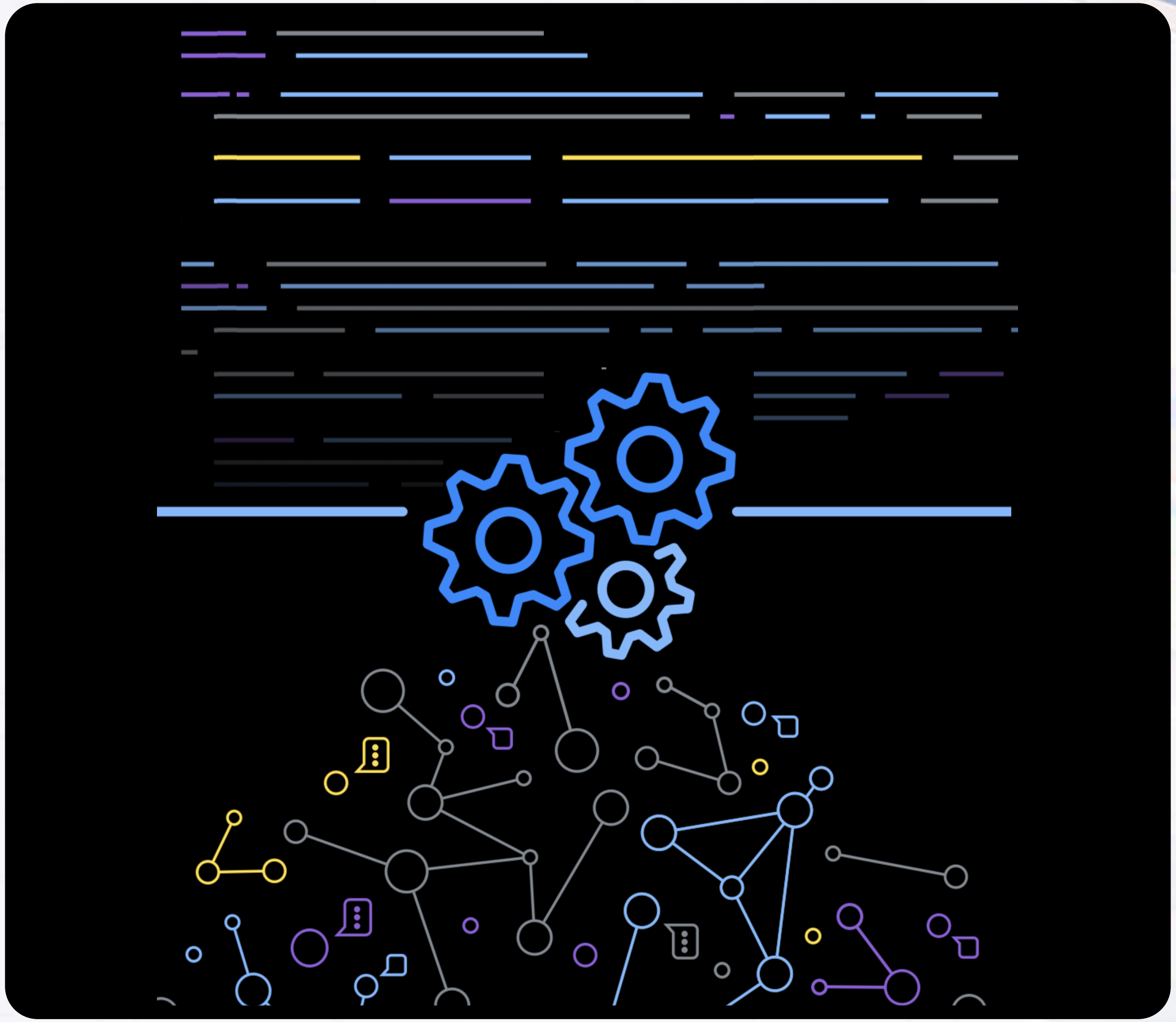
CodeQL: A revolutionary semantic code engine

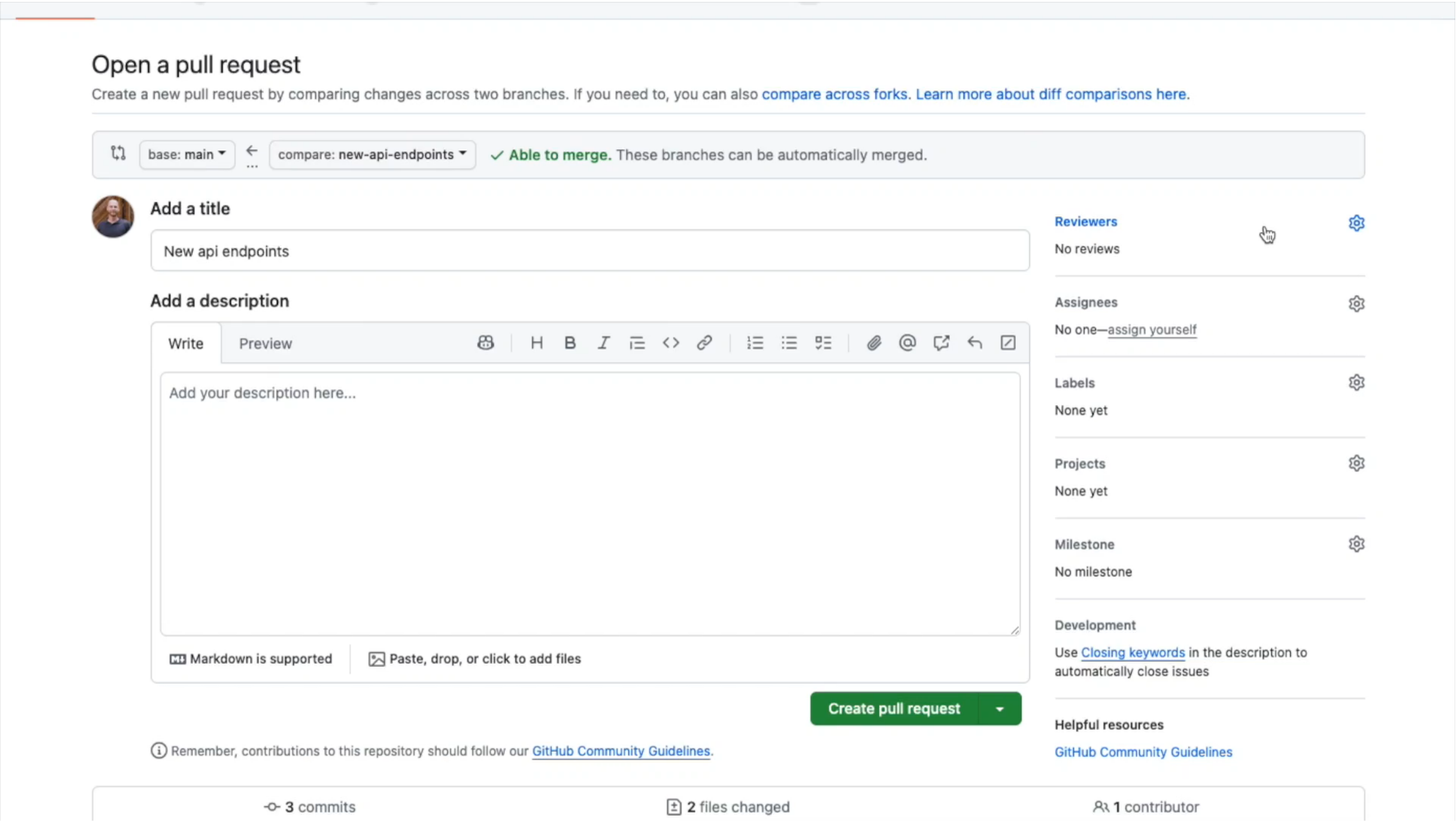
Advanced code analysis engine based on 13 years of research by a 30-person team from Oxford University.

Allows you to query your code's logic to find vulnerabilities.

Queries can be quickly customized to adapt to your specific threat topology.

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





Open a pull request

Create a new pull request by comparing changes across two branches. If you need to, you can also compare across forks. Learn more about diff comparisons here.

base: main ← compare: new-api-endpoints ✓ Able to merge. These branches can be automatically merged.

Add a title

New api endpoints

Add a description

Write | Preview

Add your description here...

Markdown is supported | Paste, drop, or click to add files

Create pull request

Remember, contributions to this repository should follow our GitHub Community Guidelines.

Reviewers
No reviews

Assignees
No one—assign yourself

Labels
None yet

Projects
None yet

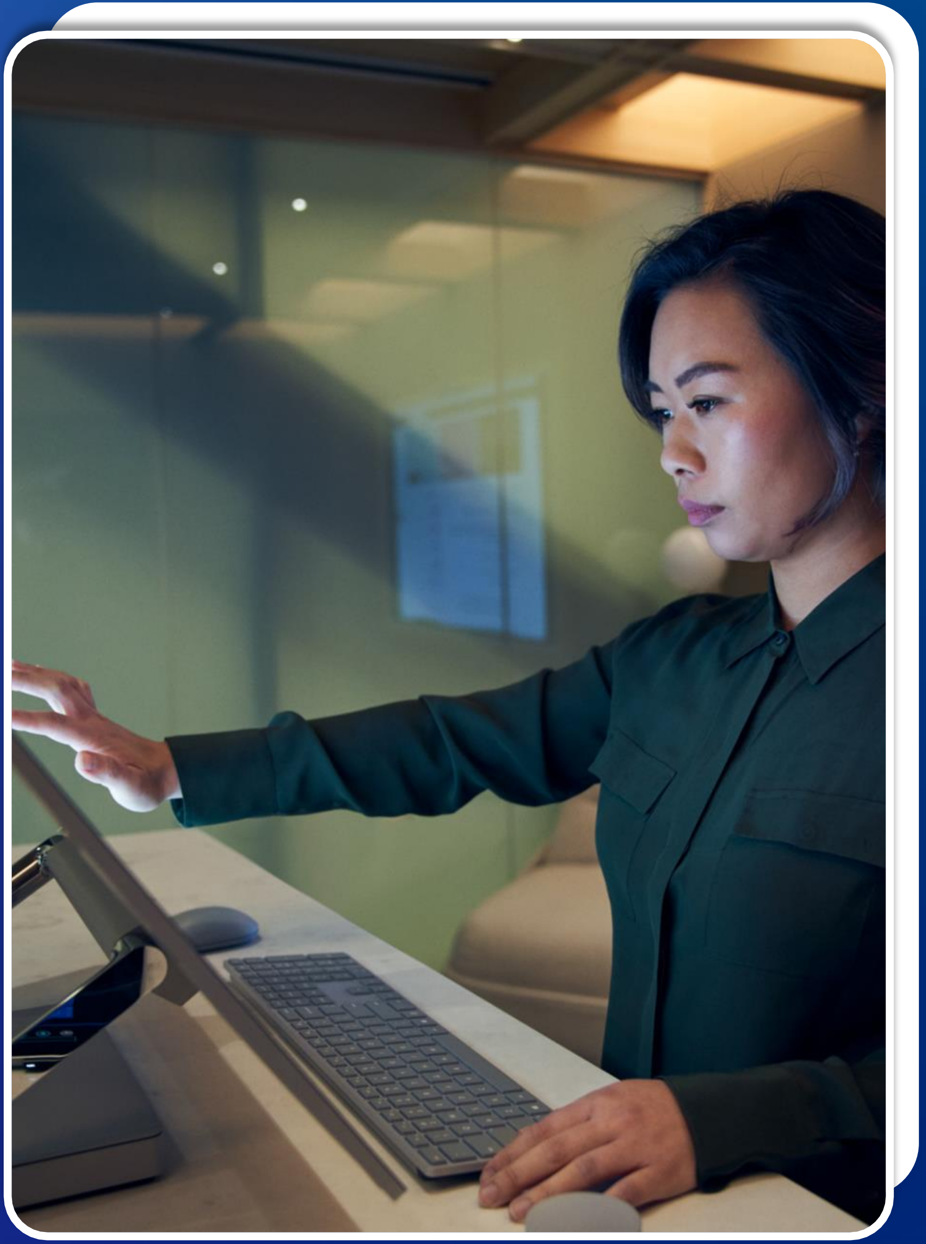
Milestone
No milestone

Development
Use Closing keywords in the description to automatically close issues

Helpful resources
GitHub Community Guidelines

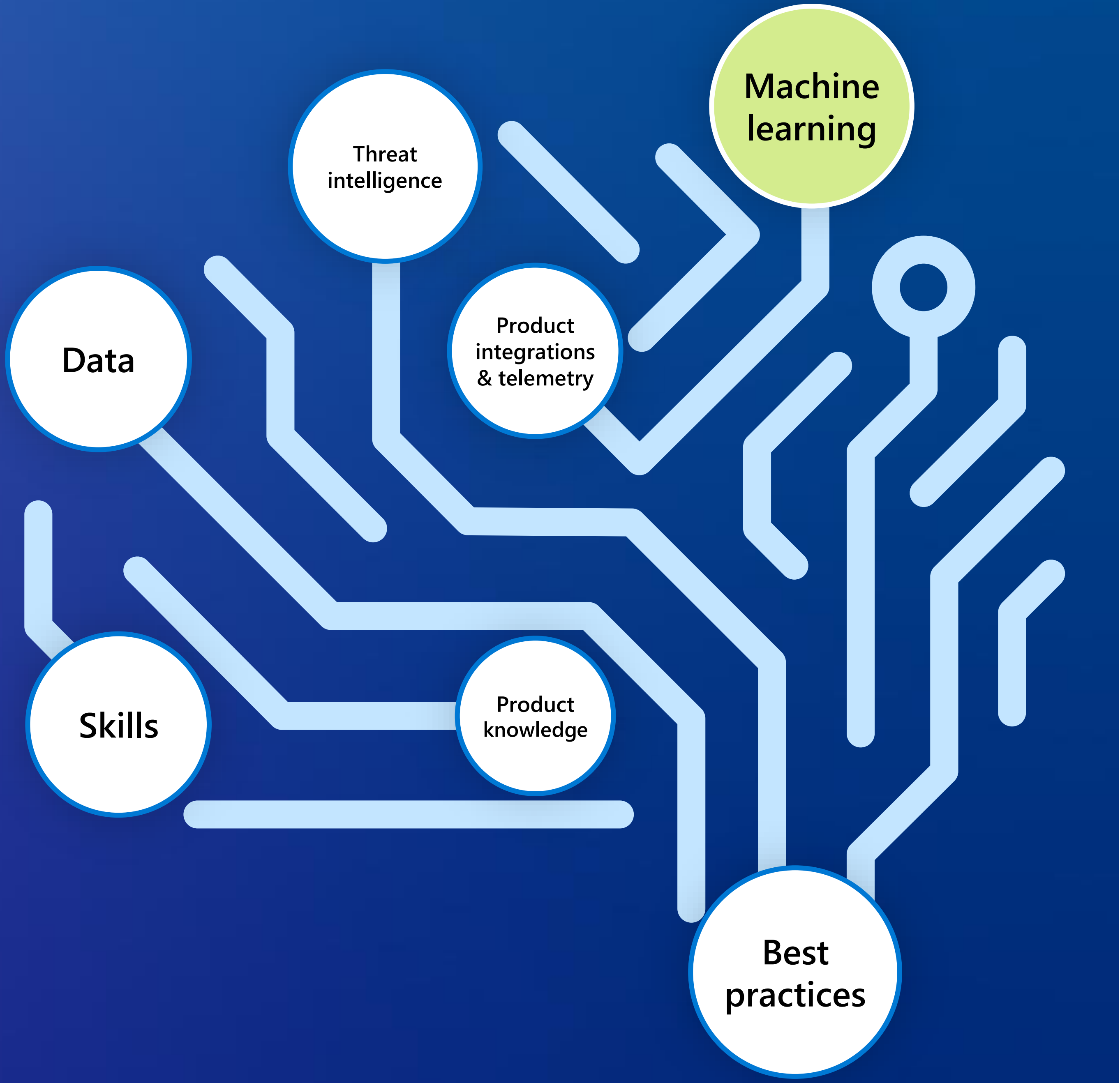
3 commits | 2 files changed | 1 contributor

Using Security Copilot to democratize security for developers

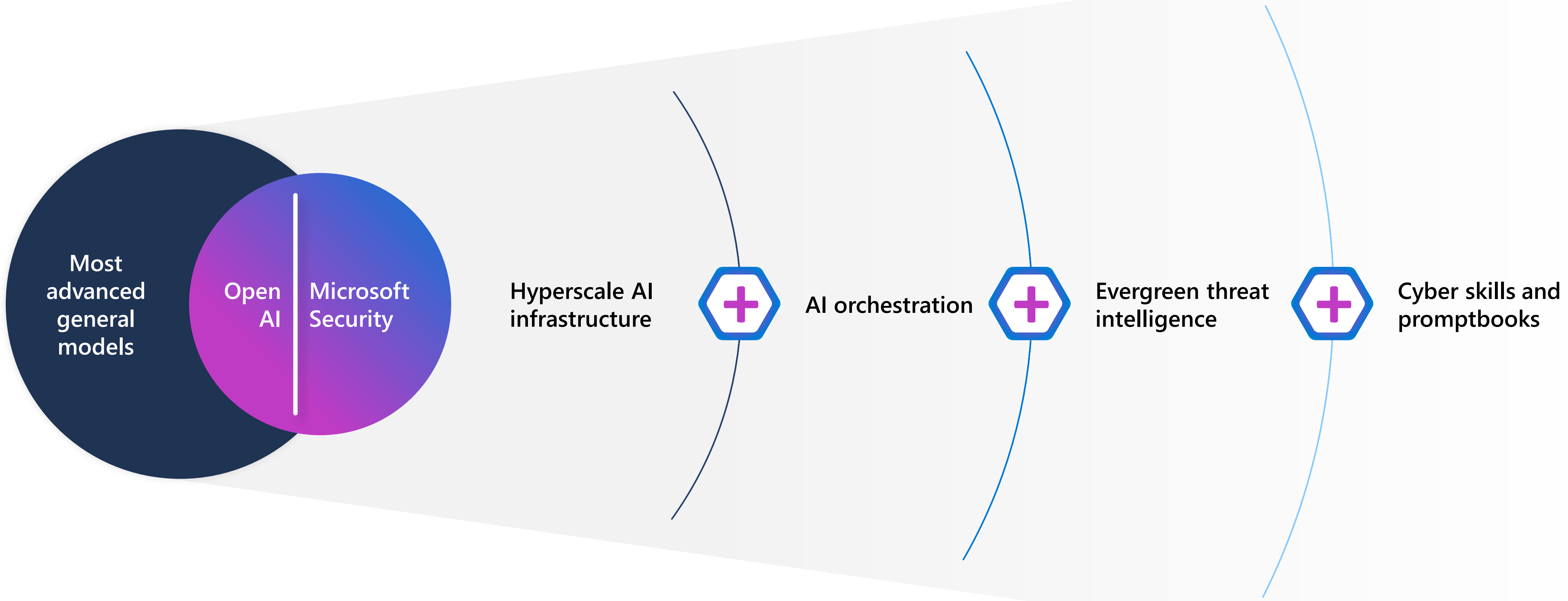


Microsoft Security Copilot

The first generative AI security product that empowers security and IT teams to defend at machine speed and scale



The Microsoft Security Copilot advantage


Most advanced general models
Open AI
Microsoft Security
Hyperscale AI infrastructure
AI orchestration
Evergreen threat intelligence
Cyber skills and promptbooks

Operated with simple natural language queries

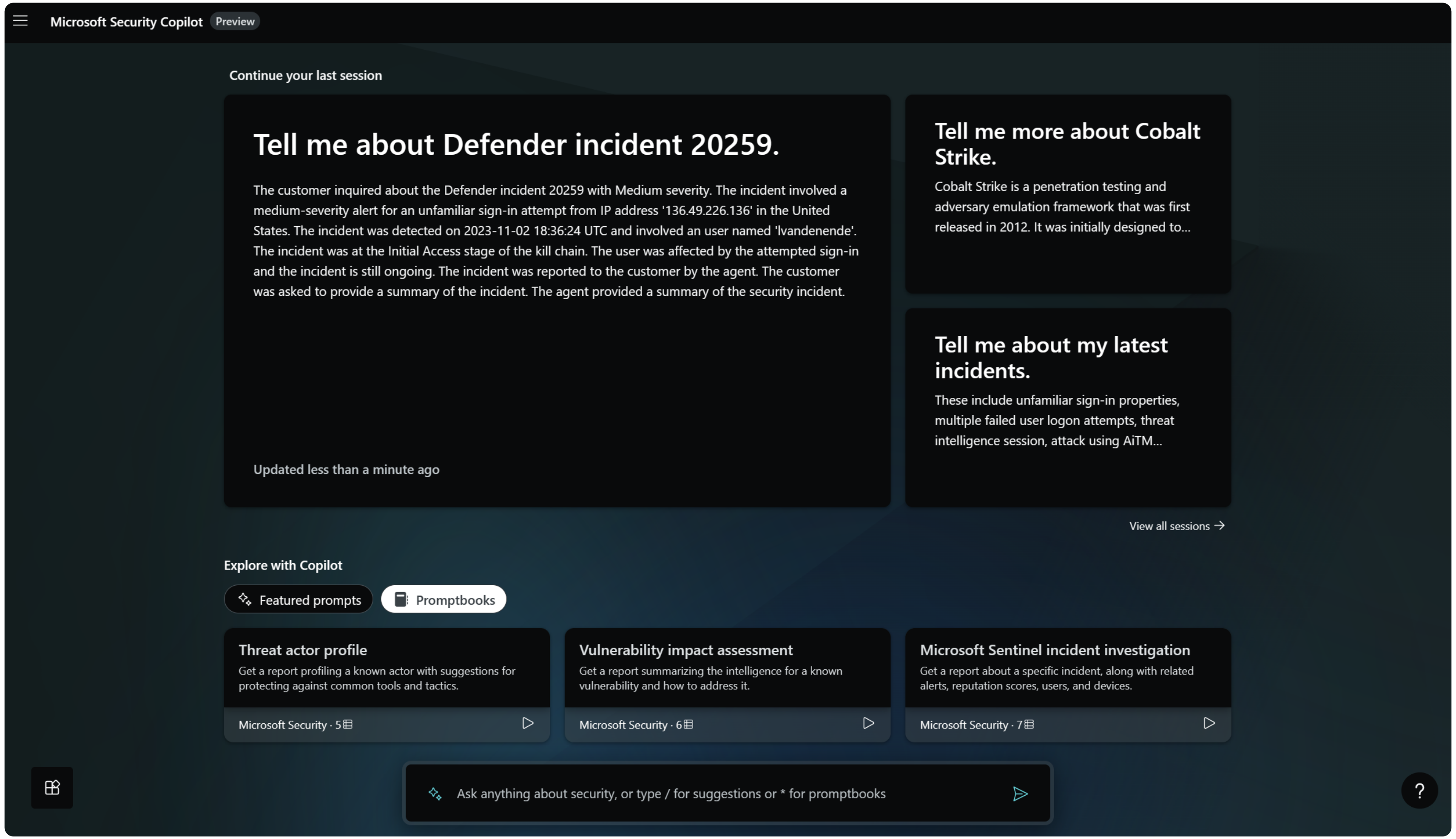
	Prompt	Planner	Build Context	Responding	Response
Human	Submits a prompt				Receives response
Security Copilot		Determines initial context and builds a plan using all the available skills	Executes the plan to get the required data context to answer the prompt	Combines all data and context and the model will work out a response	Formats the data

Microsoft Security Copilot – Video

Security Copilot

Ask anything about security

Security Copilot standalone experience



Continue your last session

Tell me about Defender incident 20259.

The customer inquired about the Defender incident 20259 with Medium severity. The incident involved a medium-severity alert for an unfamiliar sign-in attempt from IP address '136.49.226.136' in the United States. The incident was detected on 2023-11-02 18:36:24 UTC and involved an user named 'lvandenende'. The incident was at the Initial Access stage of the kill chain. The user was affected by the attempted sign-in and the incident is still ongoing. The incident was reported to the customer by the agent. The customer was asked to provide a summary of the incident. The agent provided a summary of the security incident.

Updated less than a minute ago

Tell me more about Cobalt Strike.

Cobalt Strike is a penetration testing and adversary emulation framework that was first released in 2012. It was initially designed to...

Tell me about my latest incidents.

These include unfamiliar sign-in properties, multiple failed user logon attempts, threat intelligence session, attack using AiTM...

Explore with Copilot

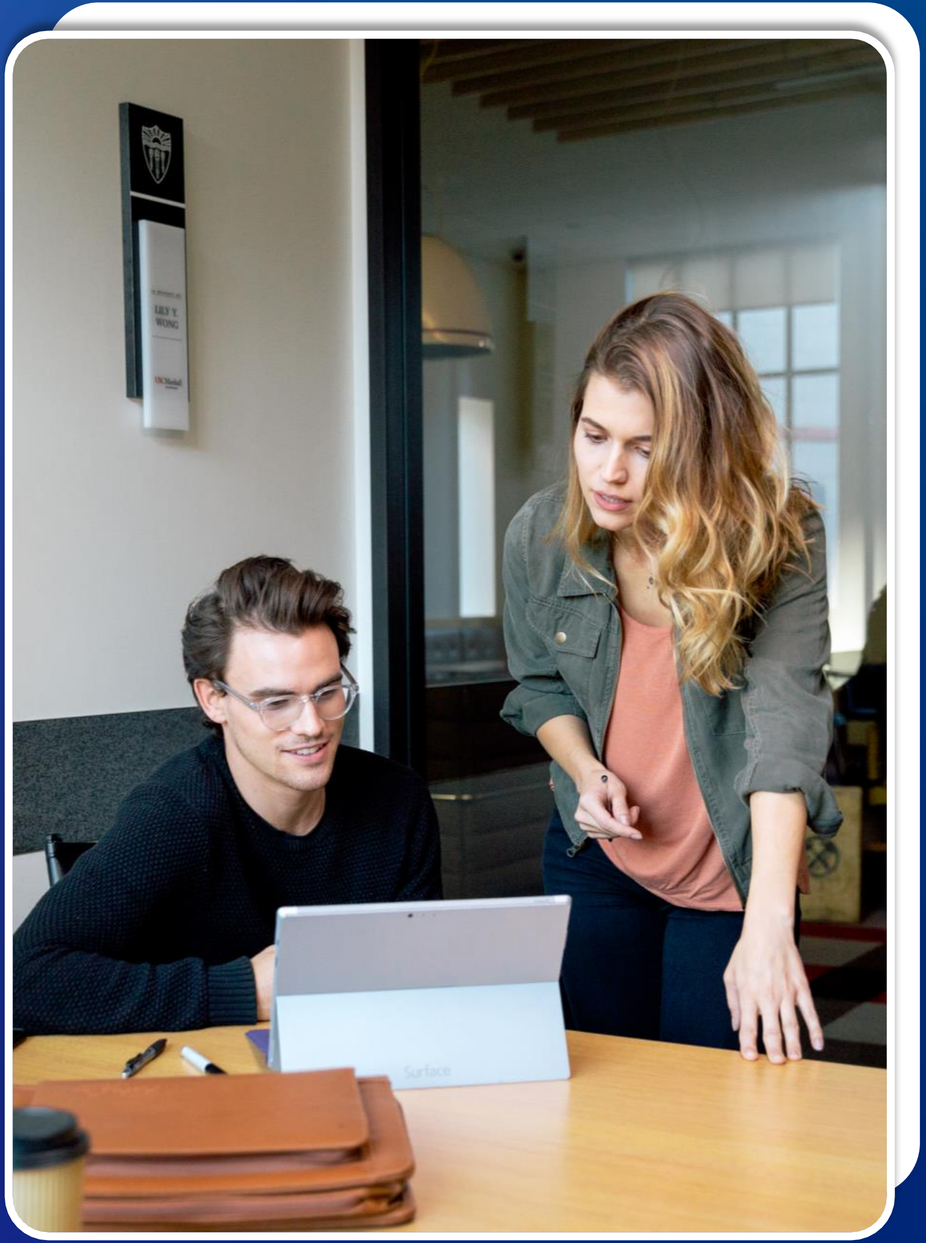
Threat actor profile
Get a report profiling a known actor with suggestions for protecting against common tools and tactics.
Microsoft Security · 5

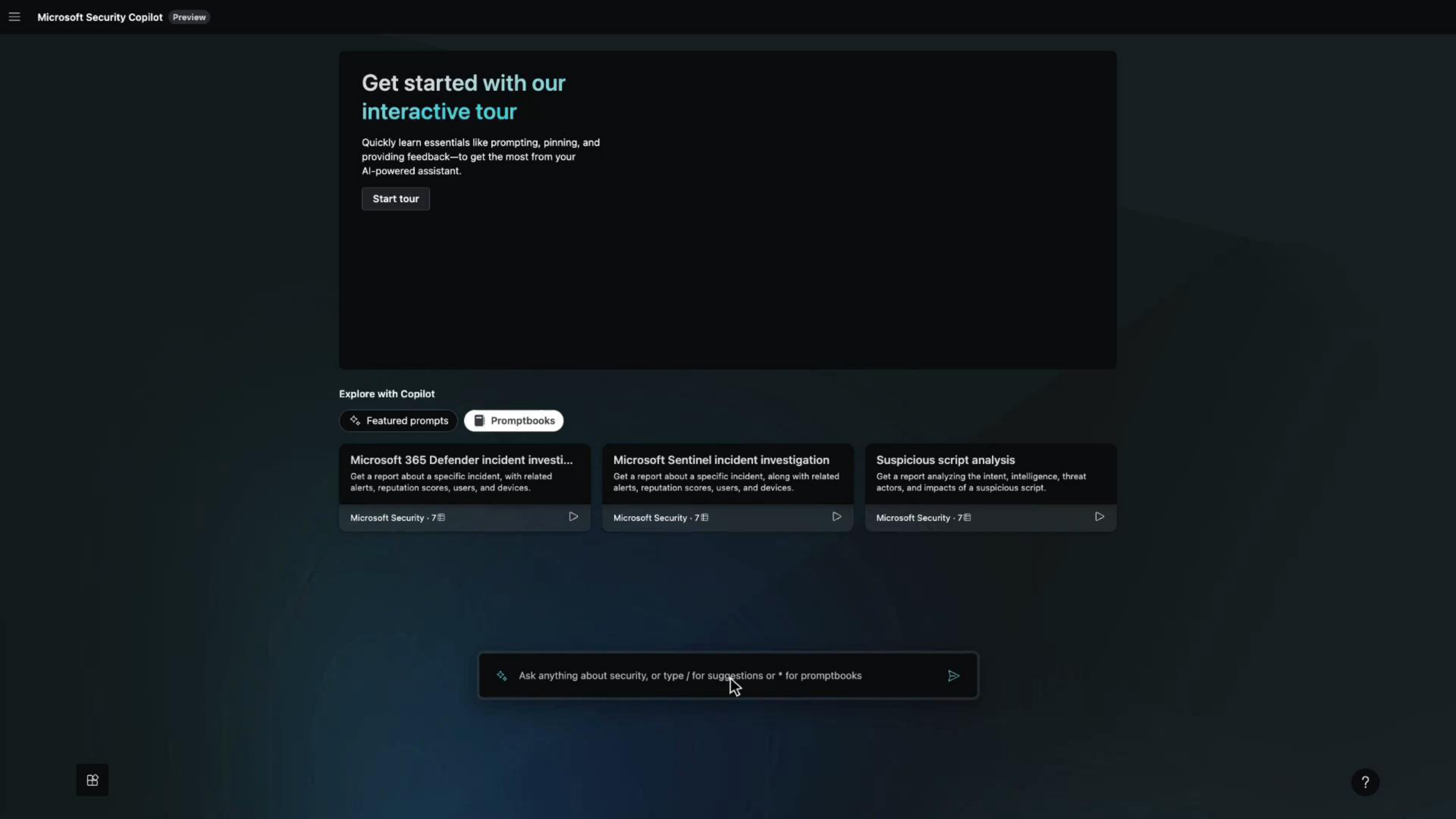
Vulnerability impact assessment
Get a report summarizing the intelligence for a known vulnerability and how to address it.
Microsoft Security · 6

Microsoft Sentinel incident investigation
Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.
Microsoft Security · 7

Ask anything about security, or type / for suggestions or * for promptbooks
?

Demo





Get started with our interactive tour

Quickly learn essentials like prompting, pinning, and providing feedback—to get the most from your AI-powered assistant.

Microsoft 365 Defender incident investi...

Get a report about a specific incident, with related alerts, reputation scores, users, and devices.

Microsoft Security · 7

Microsoft Sentinel incident investigation

Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.

Microsoft Security · 7

Suspicious script analysis

Get a report analyzing the intent, intelligence, threat actors, and impacts of a suspicious script.

Microsoft Security · 7

Ask anything about security, or type / for suggestions or * for promptbooks

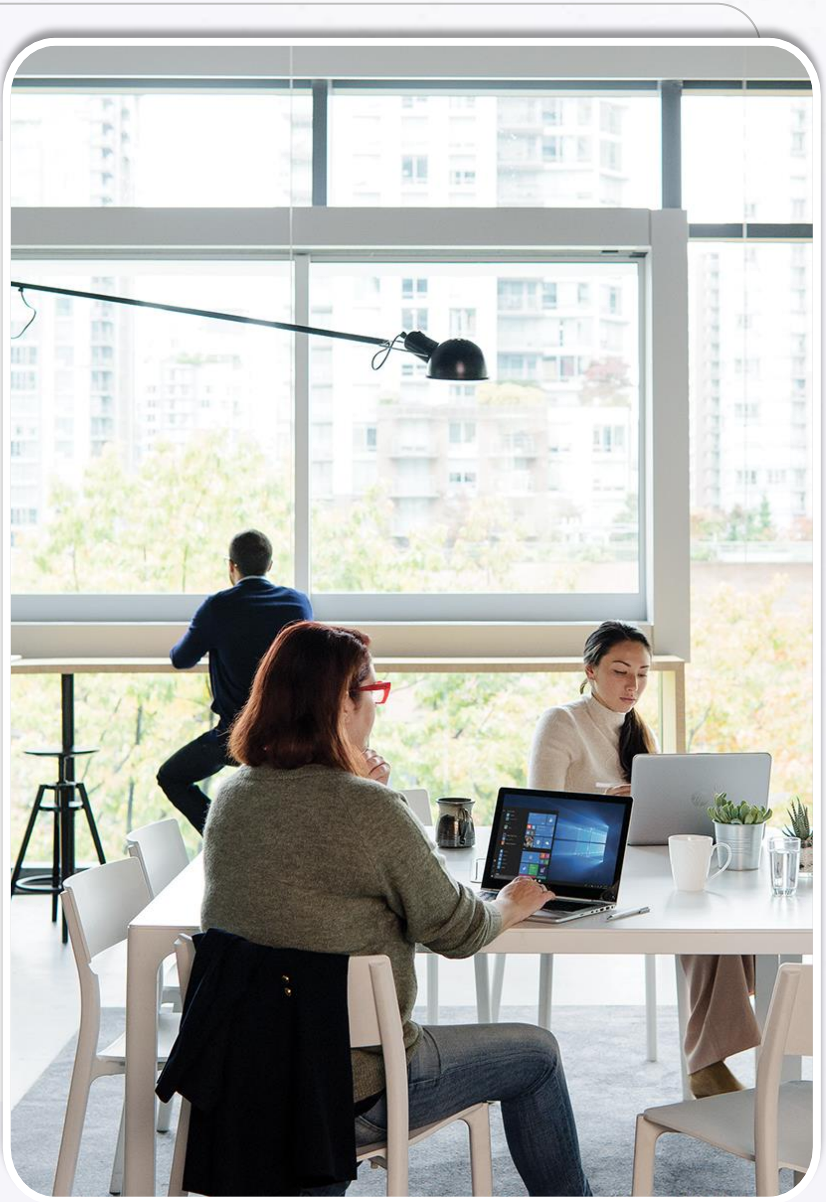
Wrap up

GHAS

- Shift left with AI-powered AppSec blog post: https://github.blog/2023-11-08-ai-powered-appsec/
- Waitlist for AI-Powered AppSec: https://github.com/features/preview/security\
- GHAS-Lab: https://github.com/skills/secure-code-game
- GHAS certifications: Examregistration.github.com

Security Copilot

- Microsoft Security Copilot documentation | Microsoft Learn



Microsoft

Register for our AI security webinar series

Copilot L33T Sp34k is a new webinar series where we interview industry experts about how to use AI securely and how organizations should use AI, like Microsoft Copilot for Security, to enhance their security.

aka.ms/copilotl33tsp34k

Let's connect!

Joylynn Kirui
Senior Cloud Security Advocate, Microsoft