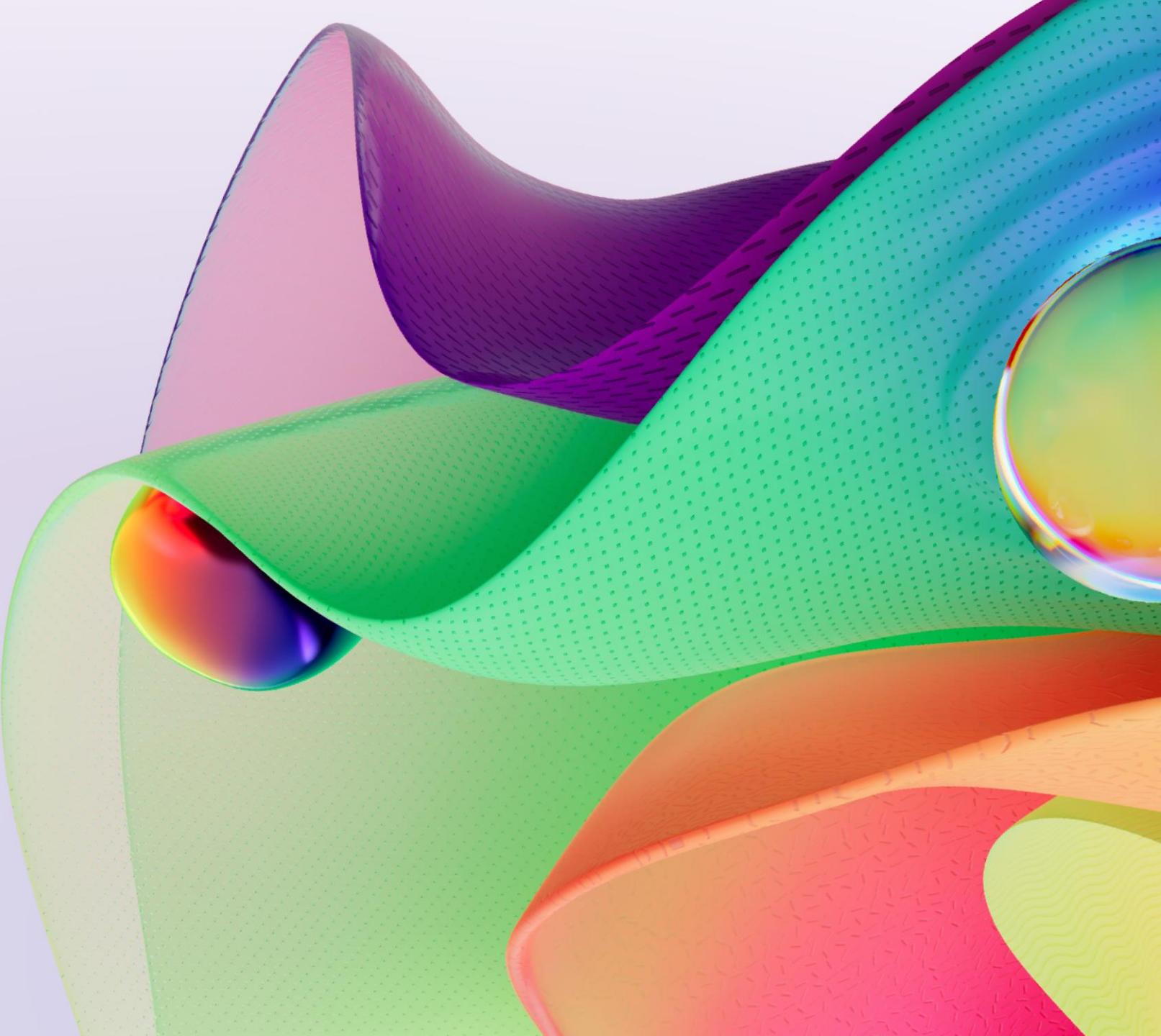




# Microsoft AI Tour

In partnership with NVIDIA.





# Future of Security with AI

Joylynn Kirui  
Senior Cloud Security Advocate  
Microsoft

X: [@joylynn\\_kirui](https://twitter.com/joylynn_kirui)



# Agenda



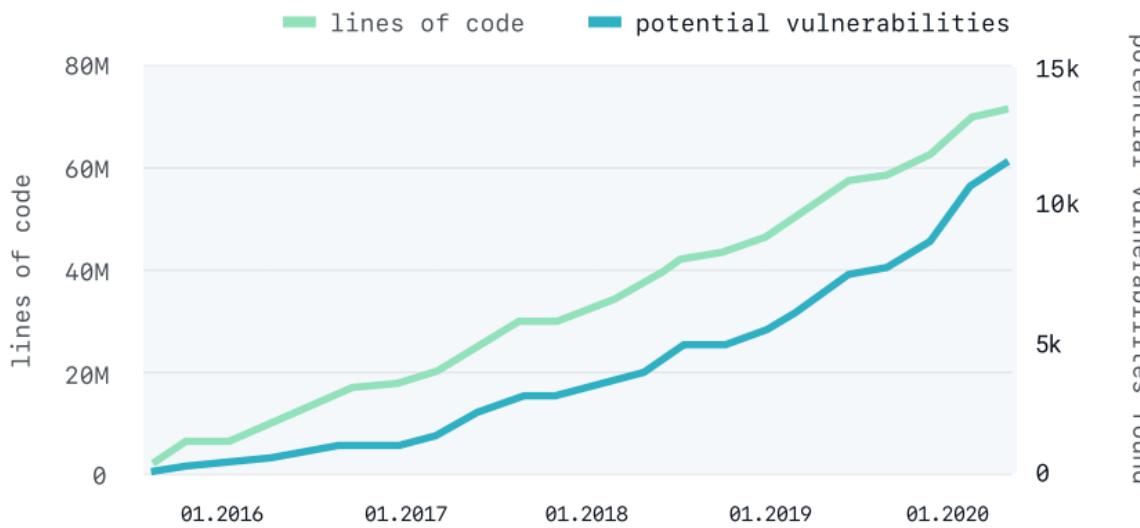
**Introduction**

**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...

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



The odds are  
against today's  
security analysts



**4,000**

Password attacks per second



**72 mins**

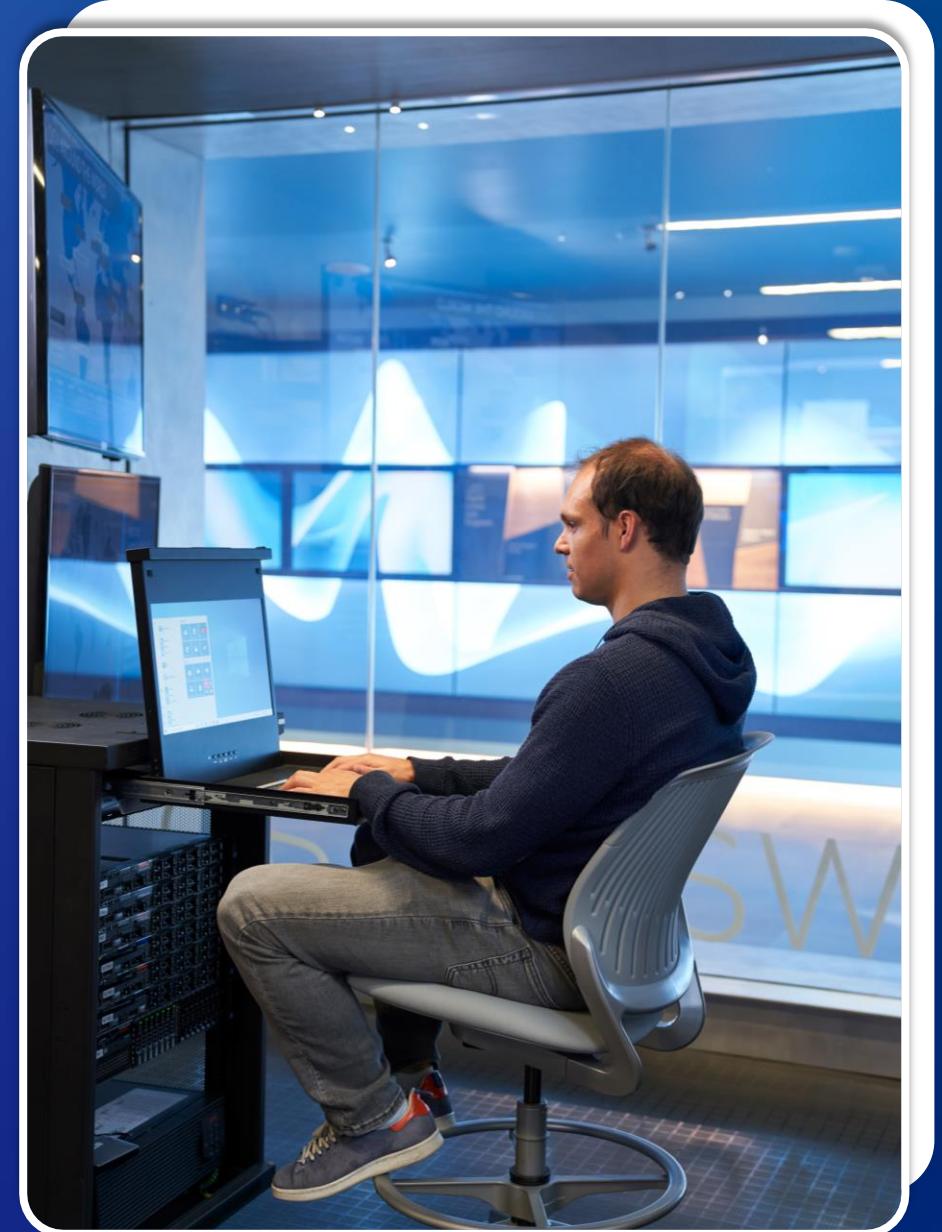
Median time for an attacker to access your  
private data if you fall victim to a phishing email



**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.

# Dependabot



Automatically raise alerts when vulnerable dependencies are detected.



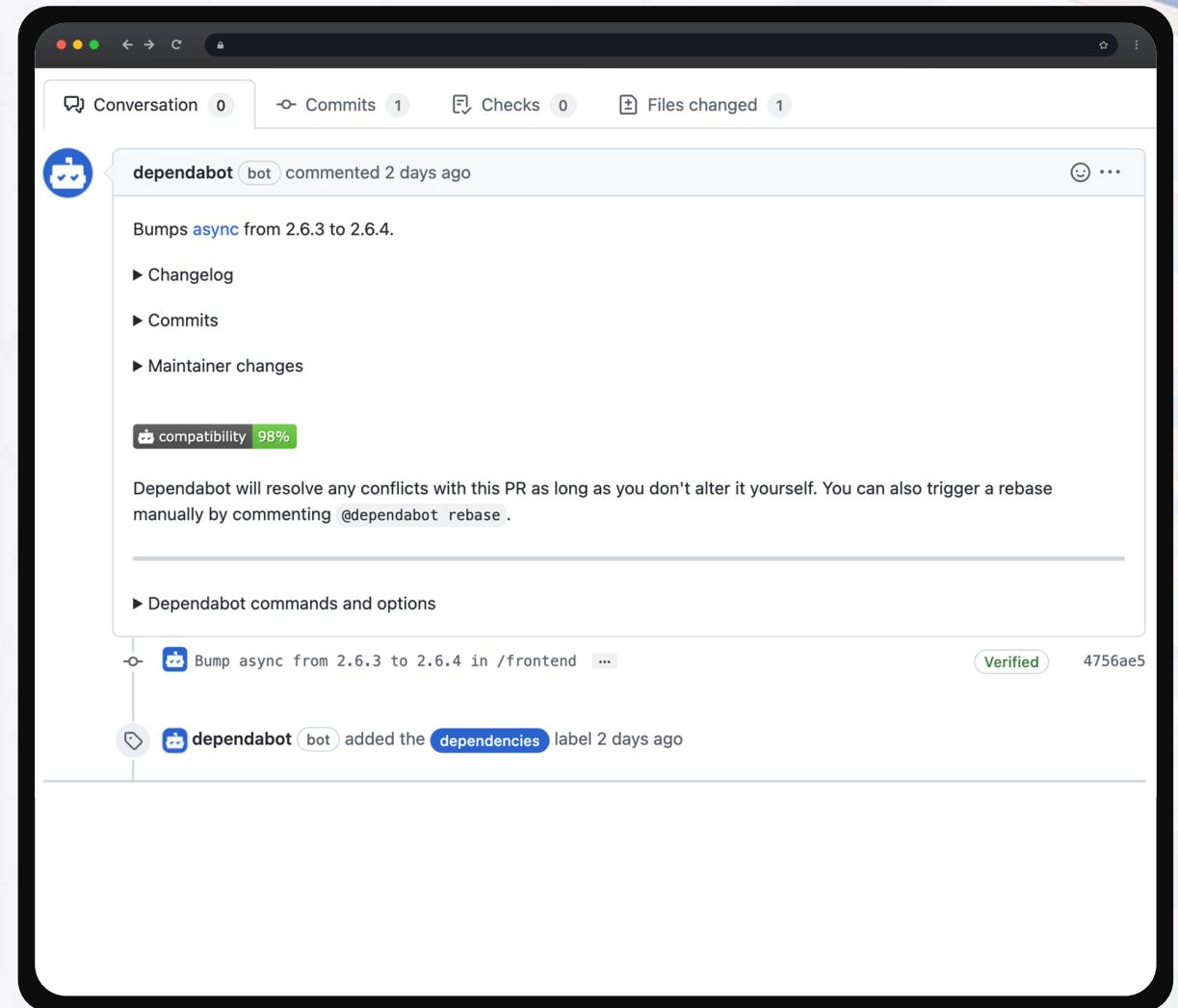
*Automatically open pull requests to fix dependency vulnerabilities.*



Notify the appropriate people about the vulnerability.



Rate the compatibility of a vulnerability patch.





# 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.

The screenshot shows the GitHub web interface for secret scanning alerts. On the left, a sidebar lists navigation options: Overview, Reporting, Policy, Advisories, Vulnerability alerts, Dependabot (11), Code scanning (2), and Secret scanning (5). The Secret scanning option is highlighted with a blue bar at the bottom. The main content area is titled "Secret scanning alerts" and features a search bar with the query "is:open". Below the search bar, there is a summary: "5 Open" and "12 Closed". A table lists five active secret scanning alerts:

Secret Type	Identifier	Last Update	Status
GitHub Personal Access Token	github_pat_11...	#18 opened now	Detected secret in secrets.txt:29
OpenAI API Key	sk-...	#17 opened 2 days ago	Detected secret in secrets.txt:27
Google API Key	AIzaS...	#16 opened 2 days ago	Detected secret in shh.txt:17
Adafruit IO Key	aio_...	#11 opened last month	Detected secret in shh.txt:4
GitHub Personal Access Token	github_pat_11A...	#10 opened last month	Detected secret in shh.txt:2

octodemo / leftrightleft-beat-bot

Type  to search | + | ○ | 🔍 | 📎 | 📄 | 🌐 | 🚙 | 🏷️

Code Issues Pull requests 1 Actions Projects Wiki Security 6 Insights Settings

leftrightleft-beat-bot Internal generated from [octodemo/beat-bot](#)

Edit Pins Watch 6 Fork 0 Star 0

main 2 Branches 0 Tags Go to file Add file Code

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

README

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.

The screenshot shows a GitHub repository page for 'dsp-testing / code-scanning-demo'. The 'Security' tab is selected. On the left, there's a sidebar with sections like Overview, Security policy, Security advisories, Dependabot alerts, Code scanning alerts (which has a red notification dot), CodeQL, and Detected secrets. The main area displays a code snippet from 'test.ts' with a yellow warning highlight around line 11. The code is:`8 */
9 const sendRedirect = async (res: ServerResponse, url: string, statusCode = 307) => {
10 res.statusCode = statusCode;
11 res.setHeader('Location', url);`

The warning message says: "Untrusted URL redirection due to user-provided value." Below the code, it says "Tool: CodeQL" and "Rule ID: js/server-side-unvalidated-url-redirection". A note explains: "Directly incorporating user input into a URL redirect request without validating the input can facilitate phishing attacks. In these 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." At the bottom, it says "First appeared in commit 1a36781 on Apr 9" and "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](#).

-o 3 commits

2 files changed

1 contributor

### 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](#)

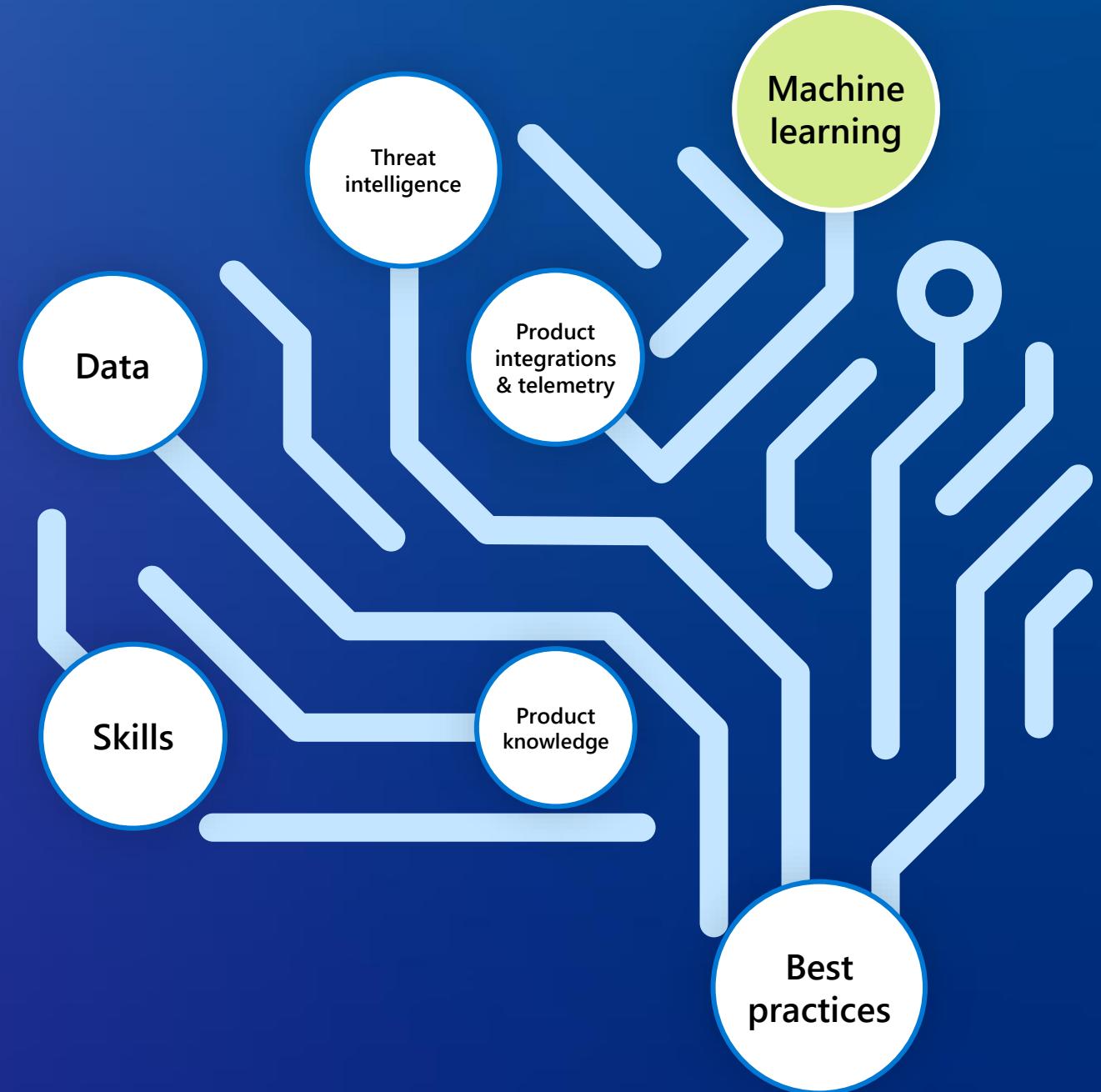
# Using Security Copilot to democratize security for developers



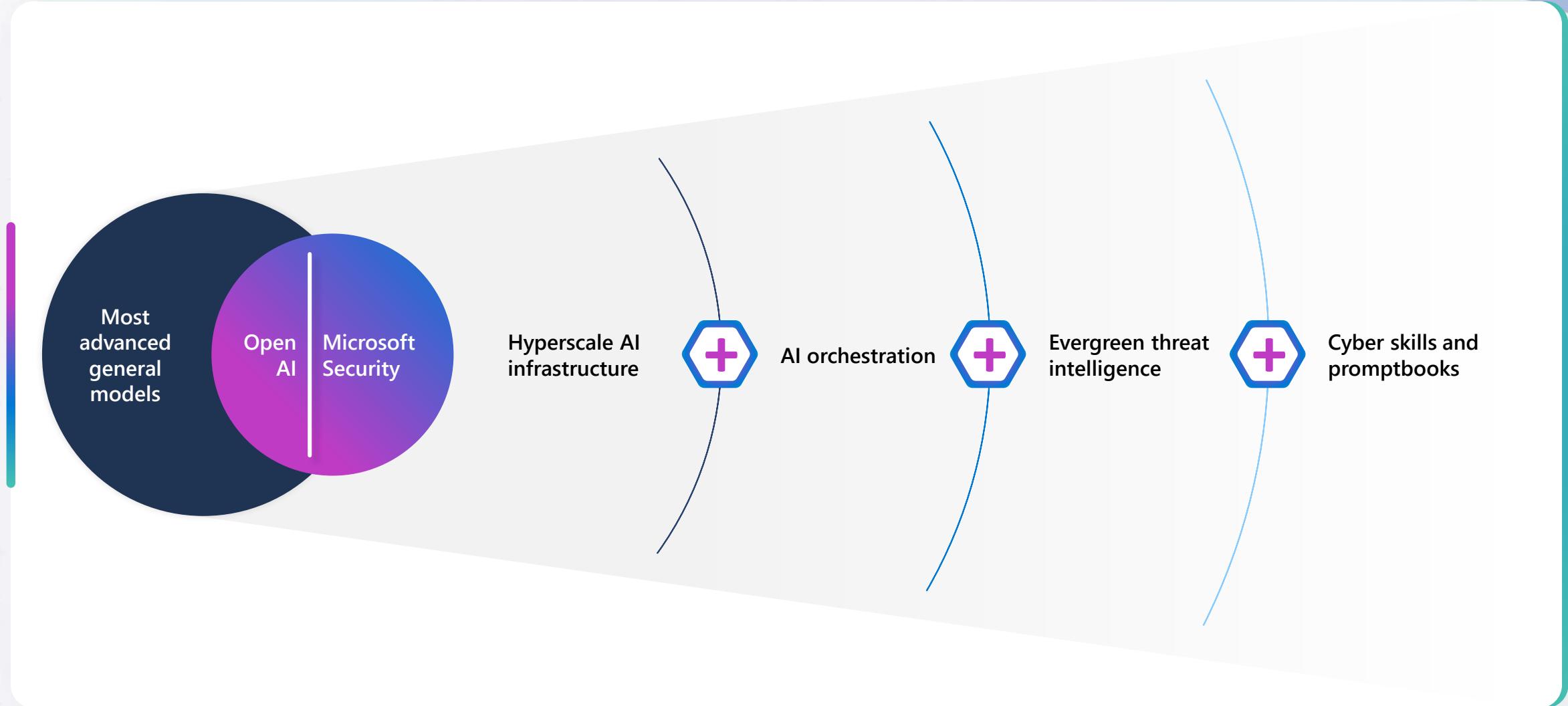


# Microsoft Security Copilot

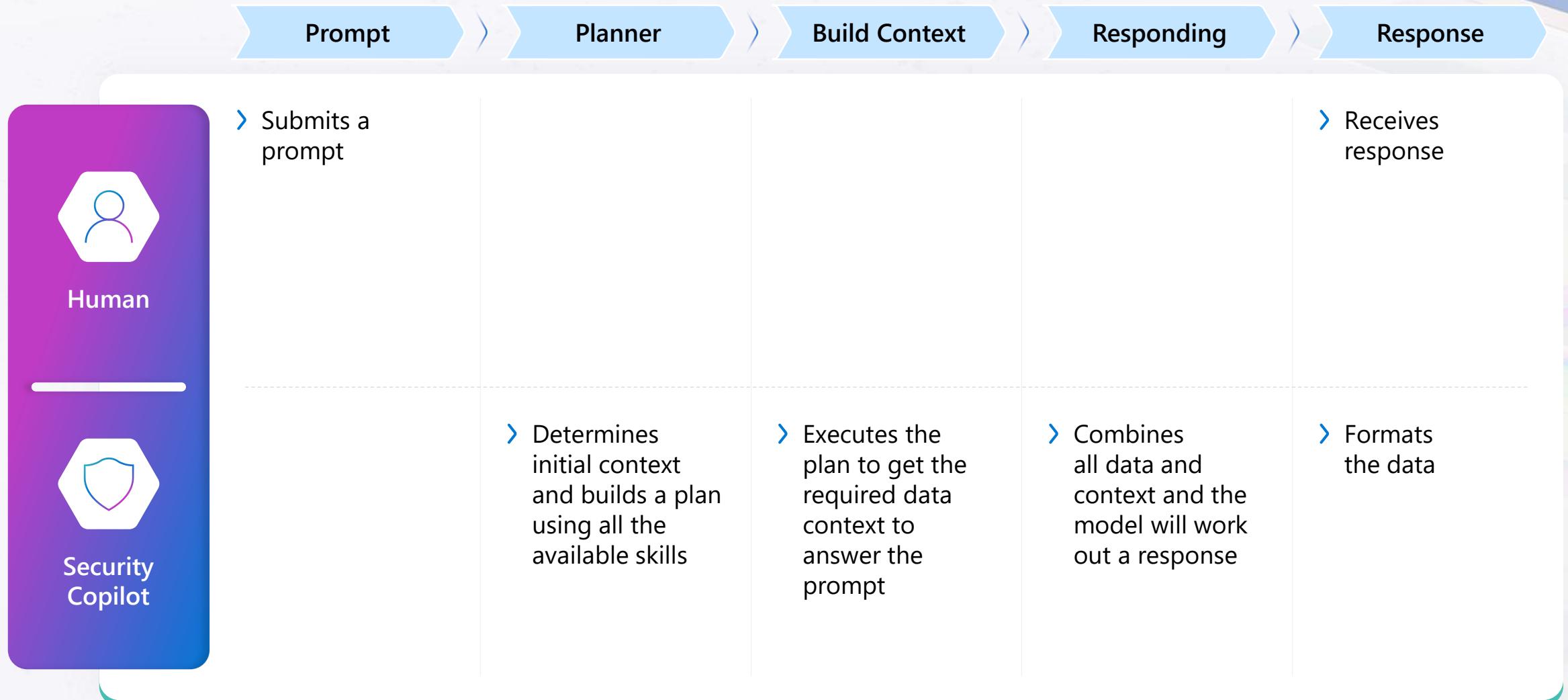
The first generative AI security product that empowers security and IT teams to defend at machine speed and scale



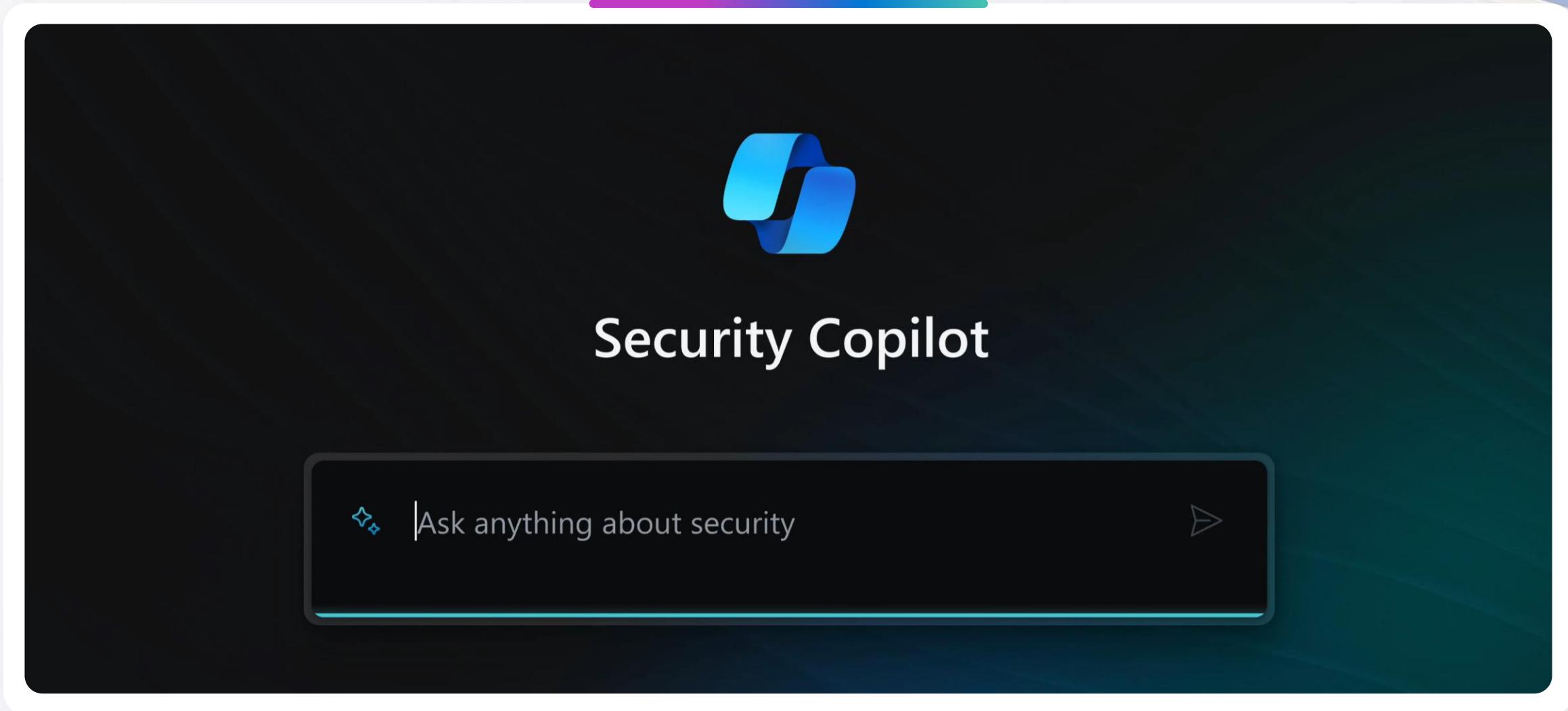
# The Microsoft Security Copilot advantage



# Operated with simple natural language queries



# Microsoft Security Copilot – Video



# Security Copilot standalone experience

The screenshot shows the Microsoft Security Copilot interface in a dark mode theme. At the top left, there's a navigation bar with three horizontal lines, the text "Microsoft Security Copilot", and a "Preview" button. Below the navigation bar, a purple and blue horizontal bar spans across the top of the main content area.

The main content area has a dark background with white text and light gray accents. At the top left of the main content area, there's a "Continue your last session" link. The main content is organized into several cards:

- 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...

At the bottom of the main content area, there's a "View all sessions →" link. Below the main content area, there's a section titled "Explore with Copilot" with two buttons: "Featured prompts" and "Promptbooks".

Three cards are listed under "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

At the bottom of the page, there's a search bar with the placeholder text "Ask anything about security, or type / for suggestions or \* for promptbooks" and a "View all sessions →" link. On the far left and right sides of the bottom bar are icons for a file and a question mark respectively.

# 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.

[Start tour](#)

Explore with Copilot

 Featured prompts  Promptbooks

### 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





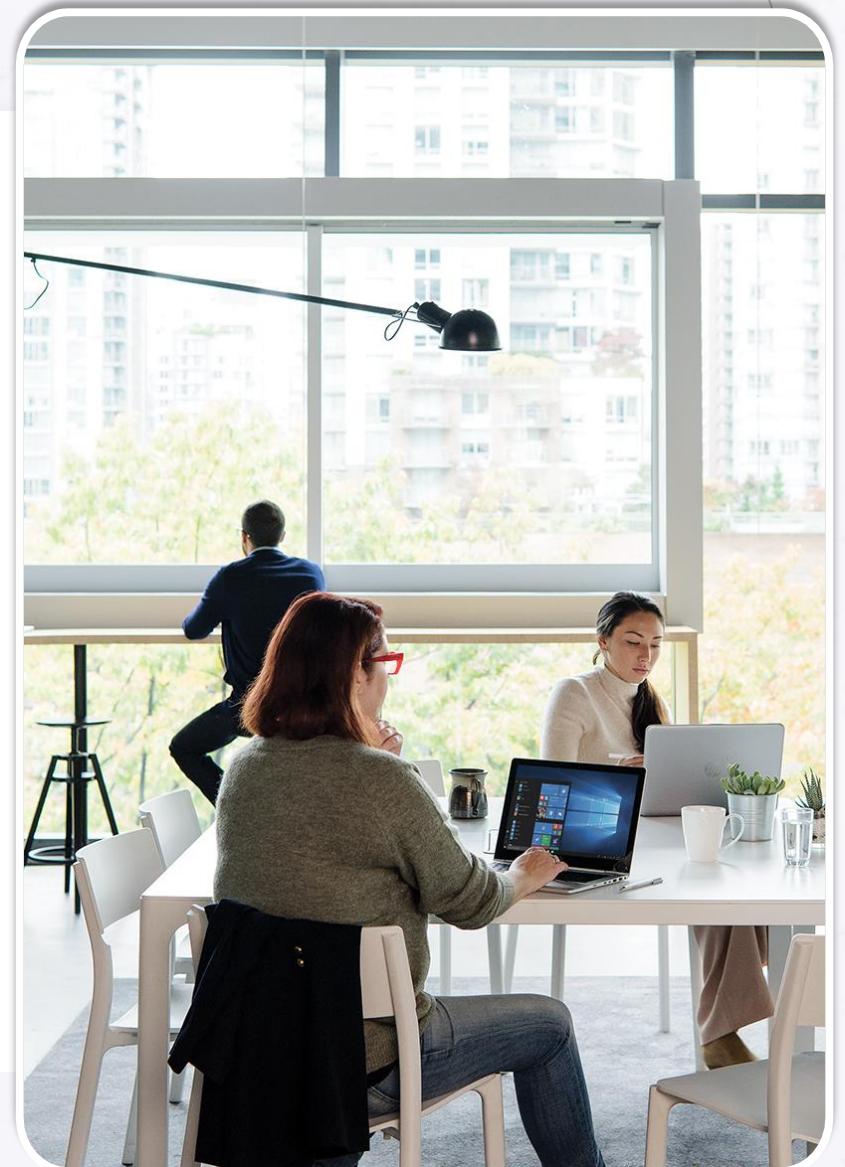
## GHAS

- 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](https://Examregistration.github.com)



## Security Copilot

- [Microsoft Security Copilot documentation | Microsoft Learn](#)





# 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](https://aka.ms/copilotl33tsp34k)





# Let's connect!

**Joylynn Kirui  
Senior Cloud Security Advocate,  
Microsoft**

