



# Microsoft Copilot for Security

An introductory deep dive



# Benefits of AI in Security – protect at machine speed

Amplify your team's impact and efficiency with guidance informed by 65 trillion daily signals.



## Catch what others miss

Summarize **vast data signals** into key insights to cut through the noise, detect cyberthreats before they cause harm, and **reinforce your security posture**.



## Outpace adversaries

Put critical **guidance and context** at analysts and admins' fingertips so they can respond **in minutes instead of hours or days**.



## Augment team expertise

Elevate teams' proficiency as **analysts and admins are empowered** to perform more advanced capabilities so expert team members can be **redirected to the hardest challenges**.



## Copilot for Security

Protect at the speed and scale of AI

*"It takes us three minutes to do a task that used to take at least a few hours"*

- Copilot for Security customer



Enable response in minutes,  
not hours



Simplify the complex with natural language prompts and easy reporting



Catch what others miss with deeper understanding of your enterprise



Strengthen team expertise with cyber skills and promptbooks

# What is Copilot for Security

Copilot for Security is a generative **AI-powered security solution** that helps increase the efficiency and **capabilities of defenders** to improve security outcomes at machine speed and scale, while remaining **compliant to responsible AI principles**.

When thinking about Copilot for Security, consider a broad reach. There are many use cases **beyond the SOC Analyst persona**.

Some include:

- IT Administrator
- Insider Risk Analyst
- Identity Access Management Administrator
- Compliance Analyst



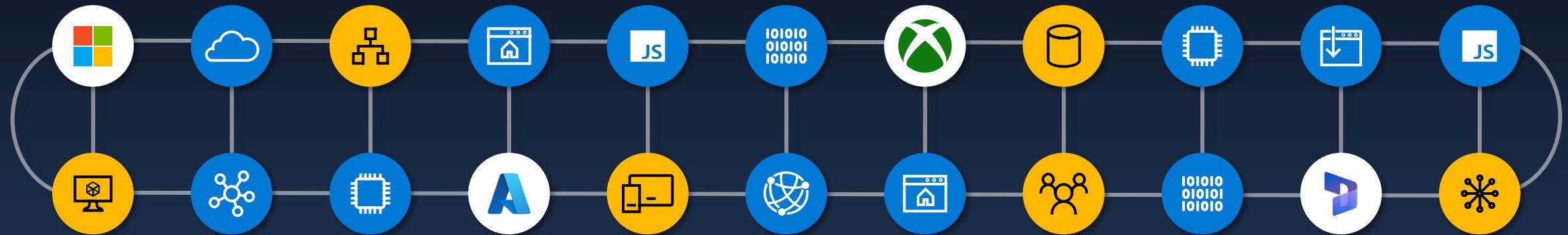
# The Copilot for Security advantage

Copilot stitches together information across all security products



# Microsoft Threat Intelligence

The industry's largest vector coverage powered by 65T daily signals



One of the  
world's largest  
clouds



Signal from 1.4B  
endpoints<sup>1</sup> across  
the planet



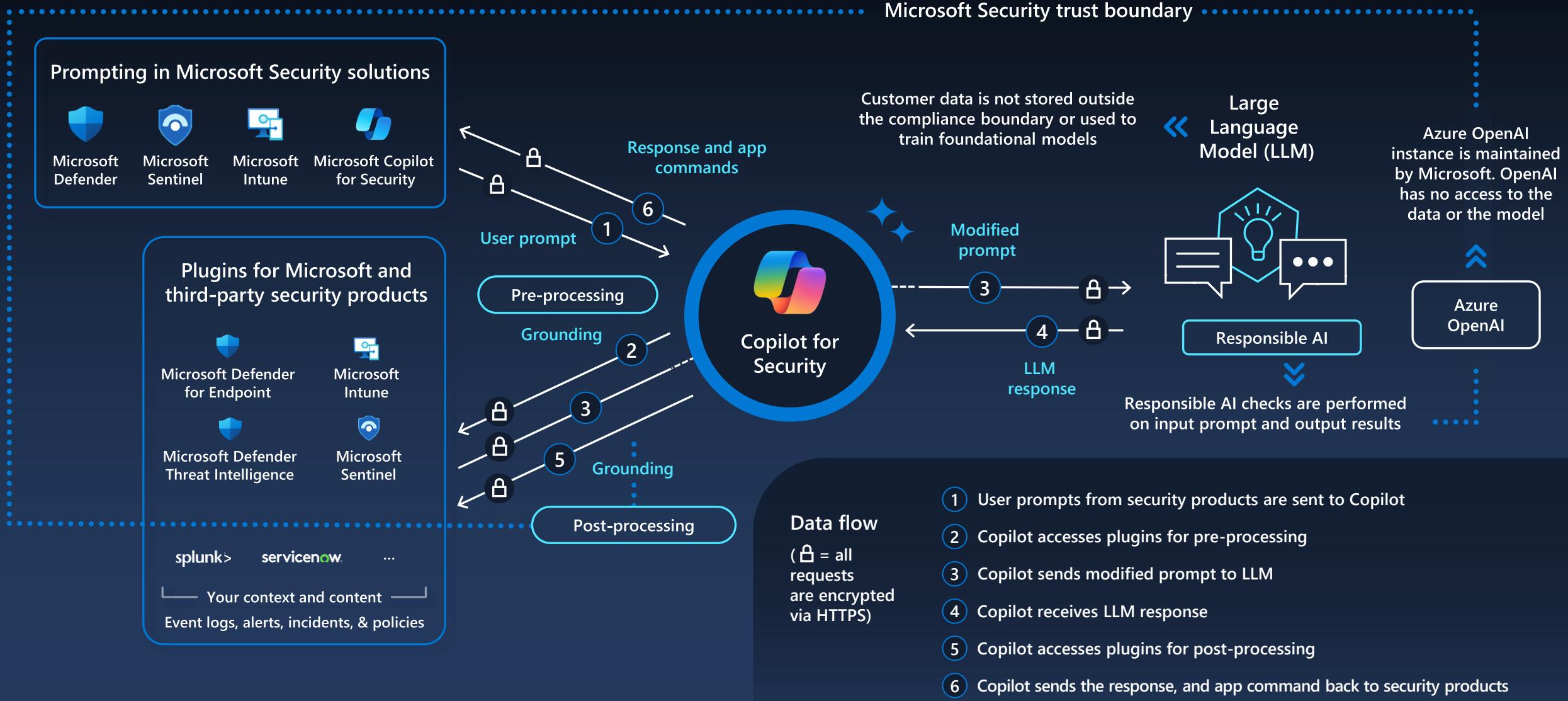
Graphing global  
internet  
infrastructure

1. "Microsoft by the Numbers". Microsoft Story Labs

# Microsoft's End-to-End Security



# Architecture – data flow for Copilot for Security



# Operated with simple natural language queries



# Architecture – example of simple prompts

"Summarize incident 15134 in Microsoft Defender into a paragraph that I can submit to my manager and create a list of entities involved."

## Goal

What is the specific security-related information you need?



"Give me information about incident 18718..."

## Context

Why do you need it and how will you use the information?



"...for a report that I can submit to my manager."

## Expectations

What format or audience do you want the response tailored to?



"Compile the information in a list, with a short summary."

## Source

Is there a plugin, known info, or data source Copilot for Security should use?

"Look in Defender incidents."

[More prompting tips](#)

# Architecture – example of simple prompts (cont.)

-  How can I improve my security posture?
-  Are any of my machines affected?
-  Summarize this incident in bullets.
-  Which alerts are being triggered the most?
-  What is log4shell?
-  Tell me about Defender incident 20259.

Tell me about Defender incident 20259. ✍️ ⌂ 🗑

> ✓ 3 steps completed 25s

Nov 2, 3:14 PM | 26.94s

Defender incident 20259 with Medium severity has a total of 1 alerts. 1 alerts were selected for summarizing the incident.

Some alerts from the incident include:

1. Severity: Medium Start time: 2023-11-02 18:36:24 Description: Unfamiliar sign-in properties relating to attempted sign-in, IP '136.49.226.136' impacting User 'lvandenende'

Here's a short summary of the incident:

The security incident occurred on 2023-11-02 18:36:24 UTC and involved a medium-severity alert. An unfamiliar sign-in attempt was detected, originating from IP address '136.49.226.136' in the United States, impacting user 'lvandenende'. The incident is at the Initial Access stage of the kill chain.

Sources

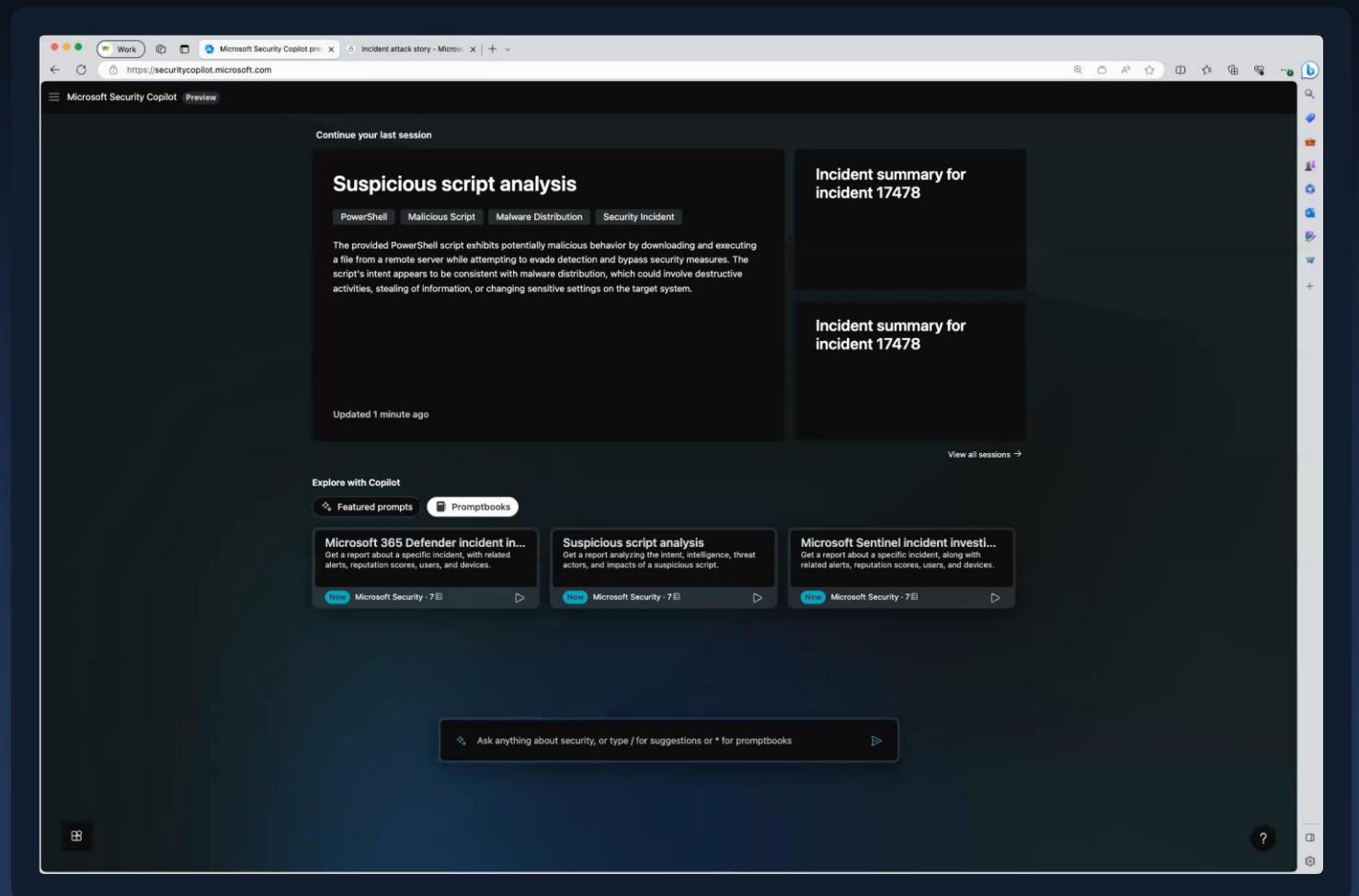
[Incident Page](#)

✓ Looks right ⌚ Needs improvement ☒ Inappropriate ⬇️ ⌂

# Demo – Copilot for Security in action

Watch how Copilot for Security **enriches and summarizes data** from your security tools to **accelerate an investigation**.

Watch the [demo](#)



# MSSP value propositions

## Augment Human Expertise

- Empowered Analysis [Script/etc...]
- Natural Language to KQL Conversion
- Guided Responses lowers skill gap training

## Increase Speed & Efficiency

- Decrease Response Triage Time
- Contextual Summarizations
- Reduce Time Consuming Routine Tasks

## Scalability, Collaboration & Reporting

- Adaptive Reallocation of Analysts
- Audience Targeted Reporting
- Agile Response & Collaboration

## MSSP Advantages

- Managed SOC Experience
- Scenario Developed Processes
- Consolidated & Adaptive Team

# Better together: Copilot for Security and MSSPs

## Knowledge:

- Learned material from training data
- What something is and how it works



## Wisdom:

- Real world experience
- Practical use of knowledge
- Ability to judge and make correct, informed decisions

The overlap of human expertise and AI provides the most benefit to customers

# Pivoting difficult customer conversations

**Copilot for Security can replace or reduce my reliance on my MSSP...**

Copilot for Security is meant to augment human expertise and not replace it. MSSPs bring a wealth of experience, talented team of experts and developed processes for handling a multitude of scenarios. This allows MSSPs to infuse their knowledge, built over time, into managed services that cannot be replicated by AI solutions that lack human driven perspective. Copilot... not Pilot...

**We have an SLA contract with our MSSP... Why do I need Copilot for Security?**

An SLA contract is only a financially backed baseline agreement of how long something can take before an action or resolution is completed by the MSSP. When it comes to threats to an organization, you want to detect, triage, respond, and remediate as quickly as possible. Any advantage that reduces the time between phases will reduce cost and damage that would have happened

**Copilot for Security is a “Double Investment” that I pay for where my MSSP benefits while their managed SOC service offering cost isn’t reduced...**

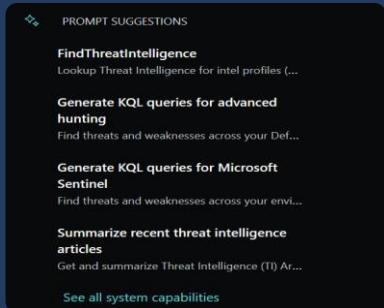
As threat actors continue to intensify their incorporation of AI, we as Defenders must also incorporate AI into our security solutions to level the playing field. Copilot for Security not only augments human expertise from the MSSP, but also provides enriched embedded experiences where the customer can benefit from the MSSP’s curated knowledge within a shared responsibility model.

# Extensibility as an MSSP – partner developed

01

## Skills

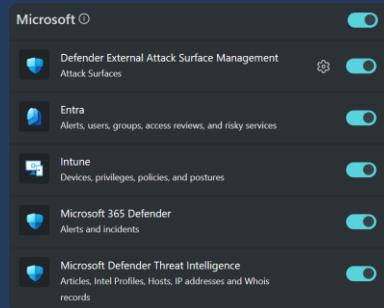
A skill is a specific capability that Copilot for Security can invoke to perform an action.



02

## Plugin

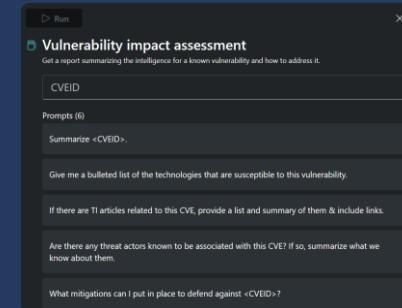
Extend and integrate services to bring more context from event logs, alerts, incidents, policies and more



03

## Promptbooks

A promptbook is like a playbook for a set of skills that can be invoked for a workflow.

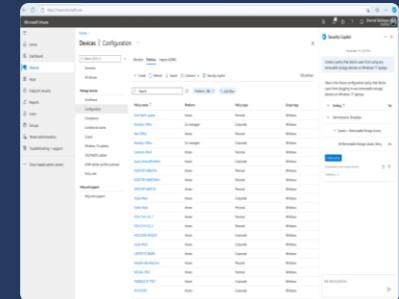


Coming soon

04

## Embedded experiences

Embed Copilot for Security UI into SaaS app/third-party admin portals.



Coming soon

# Maximizing value with Microsoft Security solutions



## Microsoft Sentinel

Collect security data and correlate alerts from virtually any source with intelligent security analytics.



## Microsoft Defender XDR

Prevent and detect cross-domain cyberattacks at the speed of AI. Copilot for Security is now embedded in Microsoft Defender XDR for early access customers.



## Microsoft Intune

Mitigate cyberthreats to devices, protect data, and improve compliance across clouds—now embedded with Copilot for Security for early access customers.



## Microsoft Defender Threat Intelligence

Understand cyberthreats and expose suspicious infrastructure with dynamic threat intelligence, now included in Copilot for Security at no additional cost.



Microsoft  
Defender



Microsoft  
Sentinel



Microsoft  
Purview



Microsoft  
Intune



Microsoft  
Entra

# Explore our delegated access roadmap for MSSPs



Available at GA

## Guest Account and Azure B2B

Customers can enable Guest Access to managed security services providers (MSSPs) by inviting the partner external user account.

Supports all workloads but requires authenticating into customer tenant individually.



Available at GA

## Granular Delegated Admin Privileges (GDAP)

GDAP capabilities allow partners to control access to their customers' workloads to better address their security concerns.

Doesn't support Microsoft Sentinel or Azure resources.



Available Post GA

## Azure Lighthouse

Cross-tenant management experiences let you work more efficiently with Azure services such as Azure Policy, Microsoft Sentinel, Azure Arc, and many more.

Only supports Azure services, most importantly Microsoft Sentinel.



Available Post GA

## Microsoft 365 Lighthouse

Cross-tenant management experiences let you work more efficiently with Microsoft 365 services.

Doesn't support Microsoft Sentinel or Azure resources.

# Partner next steps – Copilot for Security

## Partner Readiness

- [Microsoft Learn Documentation](#)
- [Learning Path](#)
- [Copilot for Security Partner Landing Page](#)
- [Microsoft Tech Community Blog](#)
- [Partner Sales & Pre-Sales Enablement Hub](#)
- [Visit our GitHub](#)

## Driving Customer Adoption

- Enable services for Plugin use
  - Microsoft Defender XDR
  - Microsoft Sentinel
  - Microsoft Entra
  - Microsoft Intune
  - Microsoft Purview
- Identify Authentication Concerns
  - On Behalf Authentication
  - Privileged Identity Mgmt
  - MDE Device Scope Groups
  - Delegated Access Models

## Extending Copilot for Security

- Custom plugins and skills
  - [GPT](#)
  - [KQL](#)
  - [API](#)
  - [Logic Apps](#)

# Set up your security capacity

Copilot for Security is a generative AI-first platform with asset mapping, tiered storage, policy services, integration services, and more. It powers all workloads of the security platform.

Azure Subscription ⓘ  
Azure subscription 1

Resource group ⓘ  
(new) SecurityCopilot

Create a new one

Capacity name ⓘ  
CIAOPS1

Prompt evaluation location ⓘ  
Australia

If this location has too much traffic, allow Copilot to evaluate prompts anywhere in the world (recommended for optimal performance).

Capacity region ⓘ  
Australia East

## Select the number of units

Security compute units provide the computing power that drives the Copilot for Security experience (USD 4 per unit).

Security compute units ⓘ  
1

Estimated monthly cost USD 2.880/month

Read more about [security compute units](#) and the recommended number based on your organization's size and probable usage.

I acknowledge that I have read, understood, and agree to the [Terms and Conditions](#)

## Security compute units ⓘ

1

Estimated monthly cost USD 2,880/month

Read more about [security compute units](#) and the recommended number based on your organization's size and probable usage.



# Setting up your security capacity ...

This might take a couple of minutes.



# Your Customer Data will be stored in Australia

This location is based on the tenant associated with this account.

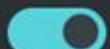
Read about how Microsoft [protects your data](#)



## Help improve Copilot

Choose whether to share data gathered from your organization's use of Microsoft Copilot for Security—including user prompts, the security information that's accessed, and Copilot's responses—with Microsoft. You can change these settings at any time.

Allow Microsoft to capture data from Copilot for Security to validate product performance using human review.



Allow Microsoft to capture and human review data from Copilot for Security to build and validate Microsoft's security AI model. ⓘ



Copilot for Security follows Microsoft's responsible AI principles and protects your Customer Data with some of the most comprehensive compliance and security controls in the industry.

Read about [Security Copilot privacy and data security](#)



# Copilot access

## Contributors

Contributors can access Copilot, but Copilot responses will vary based on existing user permissions to Microsoft Security products. After setup, owners can manage access from the role assignment page.

E

Everyone

## Owners

Contributors can access Copilot, but Copilot responses will vary based on existing user permissions to Microsoft Security products. After setup, owners can manage access from the role assignment page.

GA

Global Administrator

SA

Security Administrator

[Learn more about Copilot access](#)



# You're all set!

Your organization is ready to start using Copilot to investigate incidents, analyze suspicious scripts, summarize recent threat intelligence, and much more.

## Azure resource links

Capacity name	CIAOPS1
Subscription	
Resource group	SecurityCopilot
Location	Australia East

Share this link with your security colleagues:

[securitycopilot.microsoft.com](https://securitycopilot.microsoft.com)

Manage billing in Azure portal

# Copilot for Security standalone experience

The screenshot displays the Microsoft Security Copilot interface in a dark mode theme. At the top, a navigation bar includes a menu icon, the text "Microsoft Security Copilot", and a "Preview" button. Below the header, a "Continue your last session" link is visible.

The main content area features three 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 left, there's a "Explore with Copilot" section with "Featured prompts" and "Promptbooks" buttons. Below this are three smaller cards:

- 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 ↗

A footer bar at the bottom contains a search input field with the placeholder "Ask anything about security, or type / for suggestions or \* for promptbooks", a "View all sessions" link, and a help icon with a question mark.



How can I improve my security posture?



Are any of my machines affected?



Summarize this incident in bullets.



Which alerts are being triggered the most?



What is log4shell?



Tell me about Defender incident 20259.

Tell me about Defender incident 20259.



> (✓) 3 steps completed 25s

Nov 2, 3:14 PM | 26.94s

Defender incident 20259 with Medium severity has a total of 1 alerts. 1 alerts were selected for summarizing the incident.

Some alerts from the incident include:

1. Severity: Medium Start time: 2023-11-02 18:36:24 Description: Unfamiliar sign-in properties relating to attempted sign-in, IP '136.49.226.136' impacting User 'lvandenende'

Here's a short summary of the incident:

The security incident occurred on 2023-11-02 18:36:24 UTC and involved a medium-severity alert. An unfamiliar sign-in attempt was detected, originating from IP address '136.49.226.136' in the United States, impacting user 'lvandenende'. The incident is at the Initial Access stage of the kill chain.

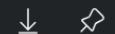
#### Sources

[Incident Page](#)

(✓) Looks right

(⌚) Needs improvement

☒ Inappropriate



Home >

## Microsoft Copilot for Security compute capacities



...



ciaopslabs (ciaopslabs.com.au)

[+ Create](#) [Manage view](#) [Refresh](#) [Export to CSV](#) [Open query](#) | [Assign tags](#) [Delete](#)

Filter for any field...

Subscription equals all

Resource group equals all

Location equals all

+ Add filter

Showing 1 to 1 of 1 records.

No grouping

List view

Name ↑↓

Type ↑↓

Resource group ↑↓

Location ↑↓

Subscription ↑↓

CIAOPS1

Microsoft Copilot for Security c... [SecurityCopilot](#)

Australia East

Azure subscription 1

...



CIAOPS1



Microsoft Copilot for Security compute capacity



Move



Refresh



Delete

Overview

Activity log

Access control (IAM)

Settings

Properties

Locks

Update

Update Security Compute Units

Automation

Tasks (preview)

Help

Support + Troubleshooting

^ Essentials

JSON View

Resource group ([move](#))

[SecurityCopilot](#)

Location

Australia East

Subscription ([move](#))

[Azure subscription 1](#)

Subscription ID

Geo

ANZ

Cross Geo Compute

Allowed

Capacity Units Provisioned

1

Tags ([edit](#))

[Add tags](#)

## Get started with Microsoft Copilot for Security.

Protect at machine speed, catch what others miss, outpace adversaries, and strengthen team expertise.



Finish setup and start using in Security Copilot

Please head to Microsoft Copilot for Security  
Portal for completing the setup

[Complete setup](#)

## CIAOPS1 | Update Security Compute Units ⚡ ⋮

Microsoft Copilot for Security compute capacity



### Update Security Compute Units

Select the number of units you want to purchase for CIAOPS1. Security compute units provide the computing power that drives the Copilot experience. [Learn more about Security Compute Units](#)

 Overview

 Activity log

 Access control (IAM)

Security compute units per hour \*

0



Estimated monthly cost \$0/month

 The min number is 1.

 Settings

 Properties

 Locks

 Update

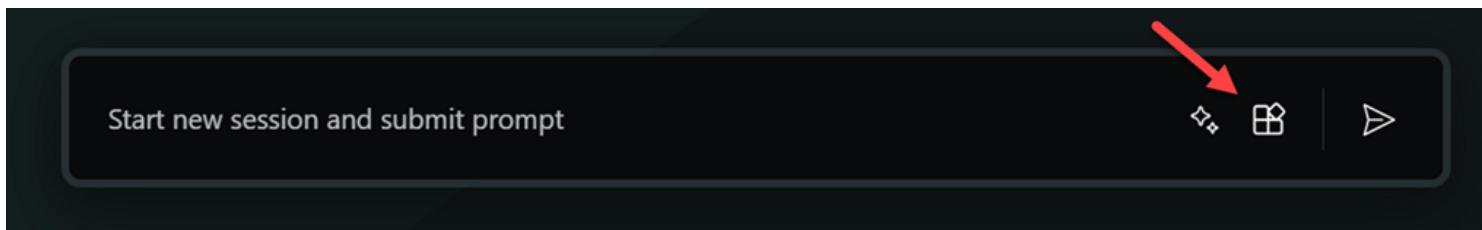
 Update Security Compute Units

 Automation

 Tasks (preview)

 Help

 Support + Troubleshooting



## Manage sources

**Plugins** **Files**

Turn on or create your own plugins to give Copilot access to the security services and websites you use. [Learn more](#)

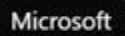
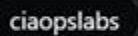
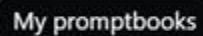
All (15) **On (7)** Off (8)

**Microsoft** ⓘ

Microsoft Defender External Attack Surface Management	<input type="checkbox"/>
Attack surfaces, vulnerable assets, and attack surface insights	
Microsoft Defender Threat Intelligence	<input checked="" type="checkbox"/>
Articles, intelligence profiles, vulnerabilities, indicators of compromise, hosts, and threat analytics	
Microsoft Defender XDR	<input checked="" type="checkbox"/>
Alerts and incidents	
Microsoft Entra	<input checked="" type="checkbox"/>
Alerts, users, groups, access reviews, and risky services	
Microsoft Intune	<input checked="" type="checkbox"/>
Devices, apps, policies, and postures	
Microsoft Sentinel (Preview)	<input checked="" type="checkbox"/>
Incidents and workspaces	
Natural language to KQL for Microsoft Defender XDR	<input checked="" type="checkbox"/>
Query-generating capability (for Defender)	
Natural language to KQL for Microsoft Sentinel (Preview)	<input type="checkbox"/>

## Promptbook library

Promptbooks contain one or more prompts that run in sequence automatically. They quickly produce custom reports and analysis using your plugins and permissions. [Learn more](#)



Name	Inputs	Plugins	Tags	Prompts	Owner
<a href="#">Microsoft 365 Defender incident investigation</a> Get a report about a specific incident, with related alerts, reputation scores, users, and devices.	DEFENDER INCIDENT ID		7	Microsoft	
<a href="#">Microsoft Sentinel incident investigation</a> Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.	... SENTINEL INCIDENT ID		7	Microsoft	
<a href="#">Suspicious script analysis</a> Get a report analyzing the intent, intelligence, threat actors, and impacts of a suspicious script.	SNIPPET	Script	8	Microsoft	
<a href="#">Threat actor profile</a> Get a report profiling a known actor with suggestions for protecting against common tools and tactics.	THREATACTORNAME	Threat Actor	8	Microsoft	
<a href="#">Vulnerability impact assessment</a> Get a report summarizing the intelligence for a known vulnerability and how to address it.	CVEID	cveid	8	Microsoft	

# End-to-end security at machine speed and scale

Microsoft Security Solutions	Available in the standalone experience	Available as an embedded experience	
 Microsoft Defender XDR	✓	✓	<b>Rapid investigation and response</b> Investigate with AI-assisted insights and quickly pivot to remediation with actionable, prioritized recommendations
 Microsoft Sentinel	✓	✓ *	<b>Scaled visibility</b> Quickly assess security posture, threats and policy or compliance gaps. Access summaries with context to understand the potential impacts.
 Microsoft Intune	✓	✓	<b>Faster troubleshooting</b> Get deep understanding of device, user, access, and app status to resolve issues quickly. Find and remediate policy issues faster with natural language prompts.
 Microsoft Entra	✓	✓	
 Microsoft Purview	✓	✓	<b>Advanced skills unlocked</b> Script analysis and natural language to KQL and KeyQL empower any team member to complete complex tasks with confidence.

\*Available as part of the Unified Security Operations Platform.

# Experiences to meet you where and how you work

## Standalone

Helps teams gain a **broader context** to troubleshoot and remediate incidents faster within Security Copilot itself, with **all use cases in one place**, enabling **enriched cross-product guidance**.

The screenshot shows the Microsoft Security Copilot interface. At the top, it says "Continue your last session". Below are three 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 'Wandenende'. 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.
- 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, there's a "View all sessions →" button and a "Explore with Copilot" section with "Featured prompts" and "Promptbooks".

## Embedded

Offers the **intuitive experience** of getting Security Copilot guidance **natively** within the products that your team members already work from and are familiar with.

The screenshot shows the Microsoft Purview Insider Risk Management dashboard. On the left, there's a sidebar with "Insider Risk Management" and various navigation options like "Overview", "Alerts", "Cases", "Policies", "Users", "Notice templates", "Adaptive protection (preview)", "Solutions", "Related", "Communication compliance", "Data Loss Prevention", and "Information barriers".

In the center, there's a card titled "(7bbc3040) Data theft by departing users" with details about the activity that generated the alert, the triggering event (HR connector imported a resignation date for this user), and user details (jdoe@discosoft.onmicrosoft.com). There are tabs for "Summary", "Activity explorer", "User activity", and "Forensic evidence".

At the bottom, there's a "Security Copilot" window with a "Natural language prompt" field containing the query "Find Mona Kane and Anne Keetings' documents and emails that contain the word 'Reader' within 2 words of '1.0', or the phrase 'MS Reader', or the word 'Reader' within 10 words of 'Microsoft'." Below it, there are buttons for "Featured prompts", "Refine", "Revert", "AI generated. Verify for accuracy.", "Generate KQL", and "KQL copied. Paste in the text box below".

 Search

Refresh

- Tenant status
- Remote Help
- Microsoft Tunnel Gateway
- Cloud PKI
- Connectors and tokens
- Filters
- Roles
- Microsoft Entra Privileged Identity Management
- Diagnostics settings
- Audit logs
- Device diagnostics
- Multi Admin Approval
- Intune add-ons
- Copilot (preview)

#### End user experiences

- Customization
- Organizational messages
- Custom notifications
- Terms and conditions

#### Let us know how Copilot is doing

Copilot can make mistakes so remember to verify the results. To help improve the experience, share your feedback with us as you use Copilot.

#### Copilot in Intune

Enabled

#### What can you do with Microsoft Copilot in Intune?

Copilot can help you with regular management tasks like policy management and troubleshooting devices. Look for Copilot throughout Intune to help you understand and manage your devices more efficiently and effectively.

[Learn more about Copilot in Intune](#)

#### How Copilot works

##### How Copilot in Intune gets answers



##### Interpreting Copilot's results



##### Monitoring usage



- [!\[\]\(df1b1fd8a5b866ab1eaba29667bb087d\_img.jpg\) Home](#)
- [!\[\]\(08a33a46a72f06c5a4dcc4b045f077b0\_img.jpg\) Dashboard](#)
- [!\[\]\(720c58fd7a58aa74fcab8c3ca386adc7\_img.jpg\) All services](#)
- [!\[\]\(1209a06d88d43914e47dd8219ec84c73\_img.jpg\) Devices](#)
- [!\[\]\(2223dc3adcfc20c782cd150ebdaaf187\_img.jpg\) Apps](#)
- [!\[\]\(df6bf403b3e0f40aad3af466acdef4e2\_img.jpg\) Endpoint security](#)
- [!\[\]\(73fd0a64d9f1e1a946d7359ae671ac39\_img.jpg\) Reports](#)
- [!\[\]\(952057dd33fa6881dda10ef3da91de76\_img.jpg\) Users](#)
- [!\[\]\(090ef0bb5b6e579f6f195229342bdf53\_img.jpg\) Groups](#)
- [!\[\]\(52c2a99d53d7237758827e426bc78520\_img.jpg\) Tenant administration](#)
- [!\[\]\(f40065e53551a6b90b3dfbd2ce7f89d7\_img.jpg\) Troubleshooting + support](#)

## Disk Encryption

BitLocker

[Summarize with Copilot](#) [Delete](#)

### Device and user check-in status

[View report](#)

#### Device assignment status

This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.

#### Per setting status

View the configuration status of each setting for this policy across all devices and users.

### Properties

#### Basics [Edit](#)

Name	Disk Encryption
Description	No Description
Platform	Windows 10 and later

#### Assignments [Edit](#)

##### Included groups

Group	Filter
No results.	

##### Excluded groups

Group
No results.

#### Scope tags [Edit](#)

Selected tags	Default
---------------	---------

#### Configuration settings [Edit](#)

#### Administrative Templates

## Copilot (preview)

AI generated insights about policy

4/1/2024, 9:59:22 AM

[Summarize this policy](#)

4/1/2024, 9:59:49 AM

The policy you're asking about is named "Disk Encryption". It's an Intune policy that primarily focuses on BitLocker settings for device encryption. Here's a summary of the key settings:

- Enforce drive encryption type on fixed data drives:** This setting is enabled and set to "Full encryption". This means that the entire drive will be encrypted when BitLocker is turned on.
- Deny write access to fixed drives not protected by BitLocker:** This setting is also enabled, which means that all fixed data drives that are not BitLocker-protected will be mounted as read-only.
- Enforce drive encryption type on operating system drives:** This setting is enabled and set to "Full encryption". This means that the entire operating system drive will be encrypted when BitLocker is turned on.
- Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later):** This setting is enabled and set to "XTS-AES 256-bit" for removable data drives, operating system drives, and fixed data drives. This means that a strong encryption method is used for these drives.
- Require Device Encryption:** This setting is enabled, which means that encryption must be turned on using BitLocker or Device Encryption.
- Allow Warning For Other Disk Encryption:** This setting is enabled, which allows UI notifications for encryption and warning prompts for other disk encryption.
- Configure Recovery Password Rotation:** This setting is set to "Refresh on for Azure AD-joined devices", which means that the Numeric Recovery Passwords will be rotated upon use for Azure AD joined devices.

Currently, there are no assignments to this policy, meaning it's not applied to any users or devices.

#### Sources:

[Microsoft Intune](#)

All generated content may be incorrect. Check it for accuracy. 

[Describe the impact of this policy on users](#) [Describe the impact of this policy on security](#) 



AI generated insights about this device

X

4/1/2024, 10:05:41 AM

Compare this device with another device

4/1/2024, 10:05:41 AM

Select another device and what you want to compare

Device 2 \* ⓘ

surfacepro-2

Comparison type \*

Discovered apps

Submit

4/1/2024, 10:06:25 AM

The device with ID e3e30cc9-0b14-4288-96fa-136ed6f1e2ae has a total of 36 discovered apps, with 12 of them being unique compared to the other device. The unique apps on this device are:

- Google Chrome, version 123.0.6312.58
- MTeams, version 23320.3021.2567.4799
- Microsoft Intune Management Extension, version 1.77.107.0
- Microsoft Visual Studio Code, version 1.85.1
- Microsoft.Advertising.Xaml, version 10.1808.3.0
- Microsoft.DesktopAppInstaller, version 2024.227.1731.0
- Microsoft.MicrosoftEdge.Stable, version 122.0.2365.59
- Microsoft.Wallet, version 2.4.18324.0
- Microsoft.WindowsAppRuntime.1.3, version 3000.882.2207.0
- Microsoft.Winget.Source, version 2024.212.956.880
- Mozilla Firefox (x64 en-US), version 121.0.1
- Notepad++, version 8.6.1 (64-bit x64)

On the other hand, the device named surfacepro-2 has a total of 34 discovered apps, with 10 of them being unique compared to the other device. The unique apps on this device are:

- Global Secure Access Client, version 1.7.669
- Google Chrome, version 123.0.6312.86

[Summarize this device](#) [Compare this device with another device](#)

Generated by Copilot for Security. [Learn more](#)

Microsoft Defender

Device inventory > surfacepro-2 > Multi-stage incident involving Credential access & Lateral movement on one endpoint

Search

Copilot

Incident summary

Apr 2, 2024 4:08 PM

The high severity incident 'Multi-stage incident involving Credential access & Lateral movement on one endpoint' occurred between 2024-04-02 04:56:38 UTC and 2024-04-02 04:58:32 UTC.

- **LateralMovement:** The incident began at 2024-04-02 04:56:38 UTC with suspicious hands-on keyboard user behavior on 'surfacepro-2' (Windows 10) by 'SuperUser'. The processes 'Taskmgr.exe' and 'lsass.exe' (running as SYSTEM) were involved.
- **CredentialAccess:** Simultaneously, there was suspicious access to the LSASS service on 'surfacepro-2' involving the same processes and user.
- At 2024-04-02 04:56:40 UTC, a process memory dump was detected on 'surfacepro-2' involving the file 'lsass.DMP' and the process 'Taskmgr.exe', impacting 'SuperUser'.
- At 2024-04-02 04:57:15 UTC, 'Leonem' malware was prevented on 'surfacepro-2', relating to the file 'AutoSaved\_93a56c43-d6ac-43f1-89ca-b7f319a299c\_Untitled1.ps1'.
- At 2024-04-02 04:57:51 UTC, suspicious 'DumpLsass' behavior was blocked on 'surfacepro-2', relating to the file 'lsass.DMP'.
- **CredentialAccess:** The incident concluded at 2024-04-02 04:58:32 UTC with a sensitive credential memory read on 'surfacepro-2' involving the processes 'Taskmgr.exe' and 'lsass.exe' (running as SYSTEM), impacting 'SuperUser'.

AI-generated content may be incorrect. Check it for accuracy.

Copilot

Manage incident

## Multi-stage incident involving Credential access & Lateral m...

Alerts (6) Assets (2) Investigations (1) Evidence and Response (4) Summary Similar incidents (0)

Attack story

High | Active | Unassigned

Alerts

Play attack story Unpin all Show all

Apr 2, 2024 3:56 PM New Suspicious hands on keyboard user behavior surfacepro-2 R SuperUser

Apr 2, 2024 3:56 PM New Suspicious access to LSASS service SURFACEPRO-2 R SuperUser

Apr 2, 2024 3:56 PM New Process memory dump surfacepro-2 R SuperUser

Apr 2, 2024 3:57 PM New 'Leonem' malware was prevented surfacepro-2

Apr 2, 2024 3:57 PM New Suspicious 'DumpLsass' behavior was blocked surfacepro-2

Apr 2, 2024 3:58 PM New Sensitive credential memory read surfacepro-2 R SuperUser

Incident graph Layout Group similar node

SURFACEPRO-2

SuperUser

2 Processes

2 Files

Communication Association

Incident details

Assigned to Unassigned Incident ID 85

Classification Not set Categories Credential access, Lateral movement, Malware, Suspicious activity

First activity Apr 2, 2024 3:56:38 PM Last activity Apr 2, 2024 3:58:32 PM

Impacted assets

Devices (1)	Risk Level	Exposure Level
surfacepro-2	High	Medium

Users (1)

SuperUser

Active alerts in this incident (6/6)

Status: All

Guided response

Apr 2, 2024 4:08 PM

Completed recommendations 0/1

Microsoft Defender

Device inventory > surfacepro-2 > Multi-stage incident involving Credential access & Lateral movement on one endpoint

Search

Copilot

Status: All

Investigation

New

Contact user  
superuser@cloudblade.onmicrosoft.com on Teams, and ask them to confirm their activity

Hi,

We noticed some unusual activity linked to your account. Specifically, we detected some actions that took place on April 2, 2024, around 4:56 AM and on March 29, 2024, around 1:16 PM. These actions involved the use of certain system tools and services that are typically not used in day-to-day operations.

To put it simply, it's as if someone was trying to access a locked room in your house. We're not sure if it was you or someone else, so we're reaching out to check.

Could you please confirm if you were using your computer at these times and if you were trying to use any advanced system tools or services? A simple 'yes', 'no', or 'don't know' would suffice.

You're welcome to provide more details if you wish. Your cooperation is greatly appreciated as it helps us ensure the security of our systems.

Best regards,  
Cyber Security Team

Copy recommendation to clipboard

All-generated content may be incorrect. Check it for accuracy.

High | Active | Unassigned

Multi-stage incident involving Credential access & Lateral m...

Copilot | Manage incident

Attack story Alerts (6) Assets (2) Investigations (1) Evidence and Response (4) Summary Similar incidents (0)

Alerts

Play attack story Unpin all Show all

Apr 2, 2024 3:56 PM New Suspicious hands on keyboard user behavior surfacepro-2 R SuperUser

Apr 2, 2024 3:56 PM New Suspicious access to LSASS service SURFACEPRO-2 R SuperUser

Apr 2, 2024 3:56 PM New Process memory dump surfacepro-2 R SuperUser

Apr 2, 2024 3:57 PM New 'Leonem' malware was prevented surfacepro-2

Apr 2, 2024 3:57 PM New Suspicious 'DumpLsass' behavior was blocked surfacepro-2

Apr 2, 2024 3:58 PM New Sensitive credential memory read surfacepro-2 R SuperUser

Incident graph Layout Group similar node

SURFACEPRO-2

SuperUser

2 Processes

2 Files

Communication Association

Incident details

Assigned to Unassigned Incident ID 85

Classification Not set Categories Credential access, Lateral movement, Malware, Suspicious activity

First activity Last activity Apr 2, 2024 3:56:38 PM Apr 2, 2024 3:58:32 PM

Impacted assets

Devices (1) Risk Level Exposure Level

surfacepro-2 High Medium

Users (1)

SuperUser

Active alerts in this incident (6/6)

Dashboard >



## Risky User Details

Reset password Confirm user compromised Confirm user safe Dismiss user risk Block user

---

Summarize Basic info Recent risky sign-ins Detections not linked to a sign-in Risk history

Summary by Copilot (Preview)

Generated by Copilot

This prompt book retrieves a Microsoft Defender incident ID and then gives detail on the entities associated with it.

**Defender incident investigation**

Specific incident, with related assets, users, and devices.

7 prompts

**SYSTEM CAPABILITIES**

Capabilities are based on the plugins you have set up.

**Analyze a script or command**

Analyze and interpret a command or script to natural language.

**Analyze security data**

Analyze, summarize, and explain security data such as event logs, and answer security questions.

**Convert Unix Timestamp**

Convert a Unix timestamp to a human readable date and time.

Start new session and submit prompt

See all system capabilities >

incident investigation  
specific incidents, assets, users, and devices.  
Prompts

**Get started using these promptbooks**

Promptbooks contain one or more prompts that help you quickly get started with Microsoft security products.

**Microsoft 365 Defender incident investigation**

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

**Microsoft Security - 7 prompts**

Get device insights, security issues, and other important information.

**MICROSOFT DOCUMENTATION**

**Ask Microsoft documentation** 

Ask questions or search for information about Microsoft security products.

**MICROSOFT ENTRA**

**Explore diagnostic log collection in Microsoft Entra**

View settings for diagnostic log collection and streaming of activity logs in Microsoft Entra ID

**Explore Microsoft Entra audit log details**

View changes to applications, groups, users, and licenses in Microsoft Entra ID

**Find group details in Microsoft Entra**

Start new session and submit prompt  

 Ask Microsoft documentation ×

Search the Purview, Intune, Defender, Entra and other Microsoft 365 product documentation



 Ask Microsoft documentation ×

How do I setup a Conditional Access policy?



# Copilot for Security elevating your security program



## Outpace adversaries

- Less time spent on low-value repetitive tasks
- Accelerated detection and response
- Critical context on incidents at analysts' fingertips



## Strengthen team expertise

- Junior analysts performing more advanced tasks
- Human expertise redirected to the hardest problems
- Guidance on processes to drive consistency



## Defend at machine speed and scale

- Reduction in mean time from detection to response
- Shift from reactive to proactive tasks
- Better understanding of risk for strategic improvements

# Outpacing adversaries to prevent threats earlier

## Resolve incidents sooner

Trim down up to 40% of time on such key activities as investigation and response, threat hunting, and threat intelligence enrichment

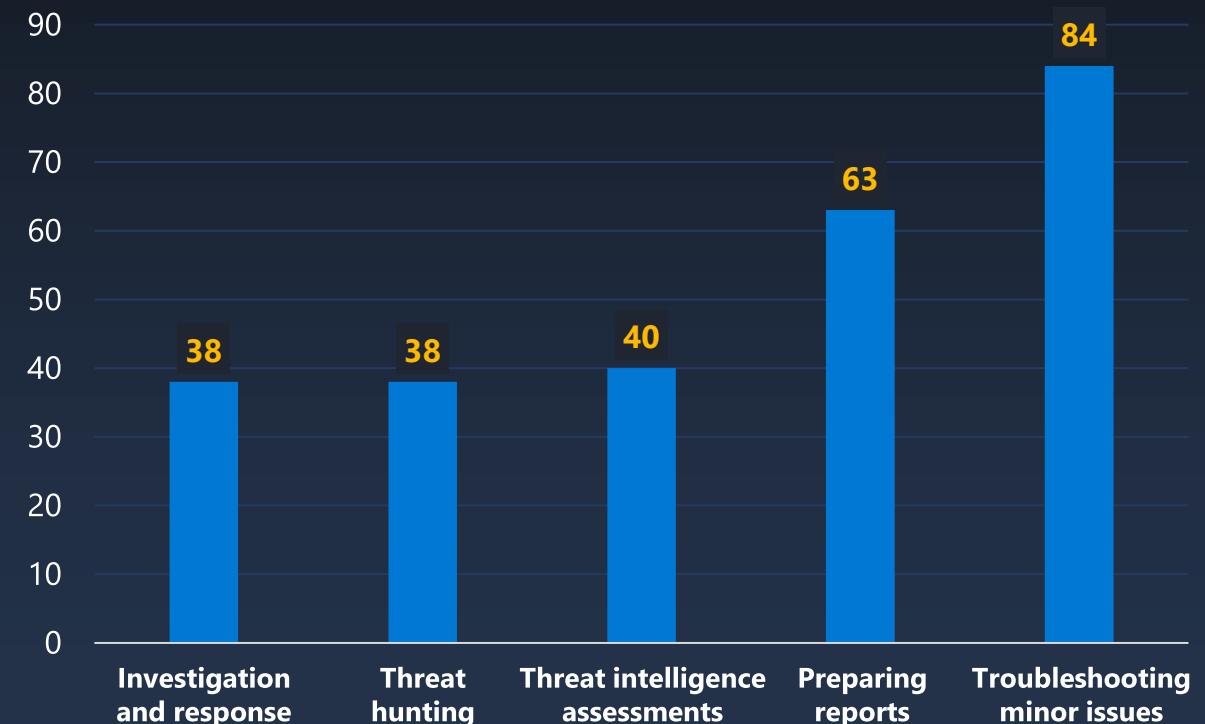
## Reduce time spent on security reporting

Drastically accelerate reporting, summarization, and visualization on any alert or incident, saving up to 63% of time on these non-mission-critical tasks

## Streamline troubleshooting

Discover issues sooner and save up to 84% of time on fixes with step-by-step guidance

% time saved on core SOC tasks



Source: Copilot for Security Private Preview customer survey conducted by Microsoft, October 2023 (N=15)

# Strengthening team expertise to focus on what matters

## Uplevel junior analyst talent

Enable less experienced team members to perform tasks normally reserved for mid to expert-level analysts, e.g., KQL data querying

## Redirect human expertise to the hardest problems

Enable your team with capabilities normally available only to the expert professionals, such as script and malware analysis

## Build consistency in operations

Get step-by-step guidance on processes such as incident response to ensure thorough response and consistent execution across team members

Copilot for Security's response level appears to be originating from...



Source: Copilot for Security response quality evaluation study by Microsoft SOC, September 2023

# Enhancing accuracy and speed

In a recent study to measure the productivity impact for “new in career” analysts, participants using Copilot for Security demonstrated **44% more accurate responses** and were **26% faster across all tasks**.

- **86%** reported that Copilot for Security helped them improve the quality of their work
- **83%** stated that Copilot for Security reduced the effort needed to complete the task
- **86%** said that Copilot for Security made them more productive
- **90%** expressed their desire to use Copilot for Security next time they do the same task



**44%**

More accurate responses



**26%**

Faster across all tasks



**86%** helped improve quality of work



**83%** reduced effort to complete the task



**86%** made them more productive



**90%** expressed desire to work with Copilot

*Source: Microsoft Copilot for Security randomized controlled trial conducted by Microsoft Office of the Chief Economist, November 2023.*

# Making organizations more secure



Increasing volume  
and sophistication of threats



Critical vulnerabilities surfaced before damage  
is done; **mean time to detect and respond**  
reduced to contain incidents sooner



Inability to adequately staff, train,  
and retain top security talent



Improved **operational efficiency** with  
increased team skills and productivity



Overworked, fatigued staff  
unable to focus on what matters



Shift **from reactive to proactive**: ability to  
focus on high priority problems and critical tasks



Reactive security operation poorly  
adjusted to risk and business priorities



Improved understanding of **business risk**  
and **executive and board-level reporting**

