# Introduction to Microsoft Copilot for Security

Beata Zalewa, Microsoft Community Łódź, 10.10.2024

zalnet

# About me

Security Architect

Consultant

Microsoft Certified Trainer

AI & Cybersecurity Practitioner

Developer

Freelancer

Azure

Azure @ ♥

aws

Google Cloud

1 Husband

1 Daughter

2 cats

2 dogs

Detective stories

Photography

zalnet
BEATA ZALEWA

https://www.linkedin.com/in/beatazalewa/

beata@zalnet.pl

https://zalnet.pl/

# Solution overview

What is **Microsoft Copilot for Security**?

Microsoft 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.

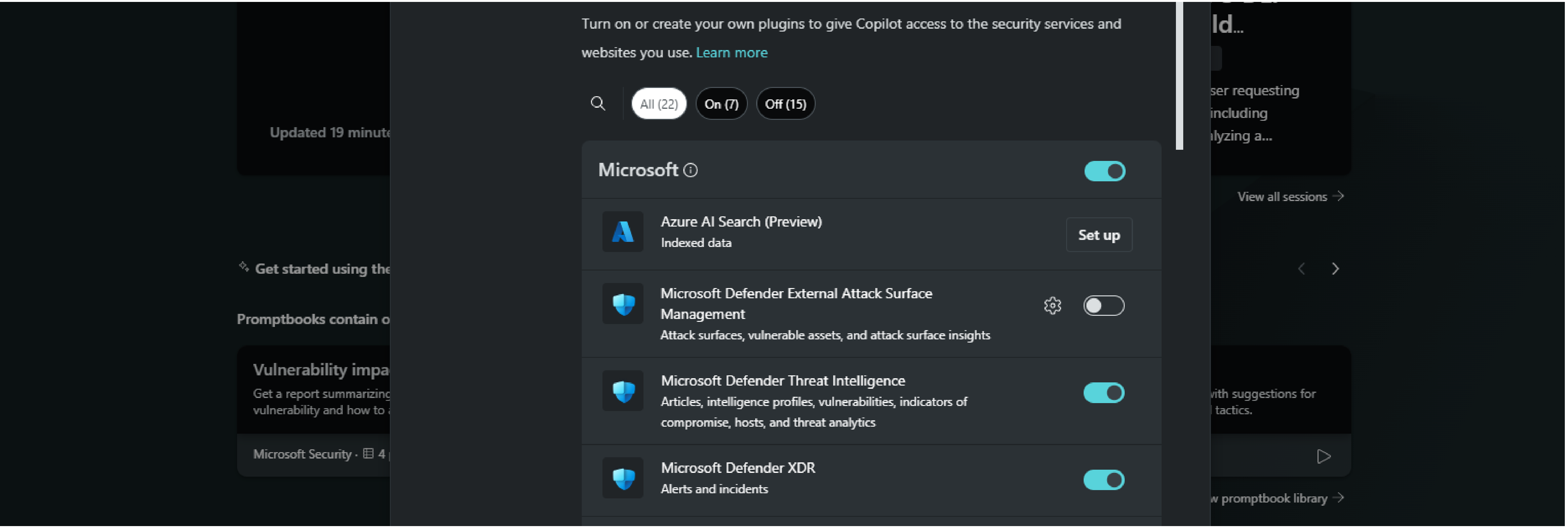
Copilot for Security provides a natural language, assistive copilot experience.

Copilot for Security helps support security professionals in end-to-end scenarios such as incident response, threat hunting, intelligence gathering, and posture management.

The solution leverages the full power of **OpenAI** architecture to generate a response to a user prompt by using security-specific plugins, including organization-specific information, authoritative sources, and global threat intelligence.

By using plugins as data point sources, security professionals have wider visibility into threats and gain more context and have the opportunity to extend the solution's functionalities.

# Copilot for Security and OpenAI



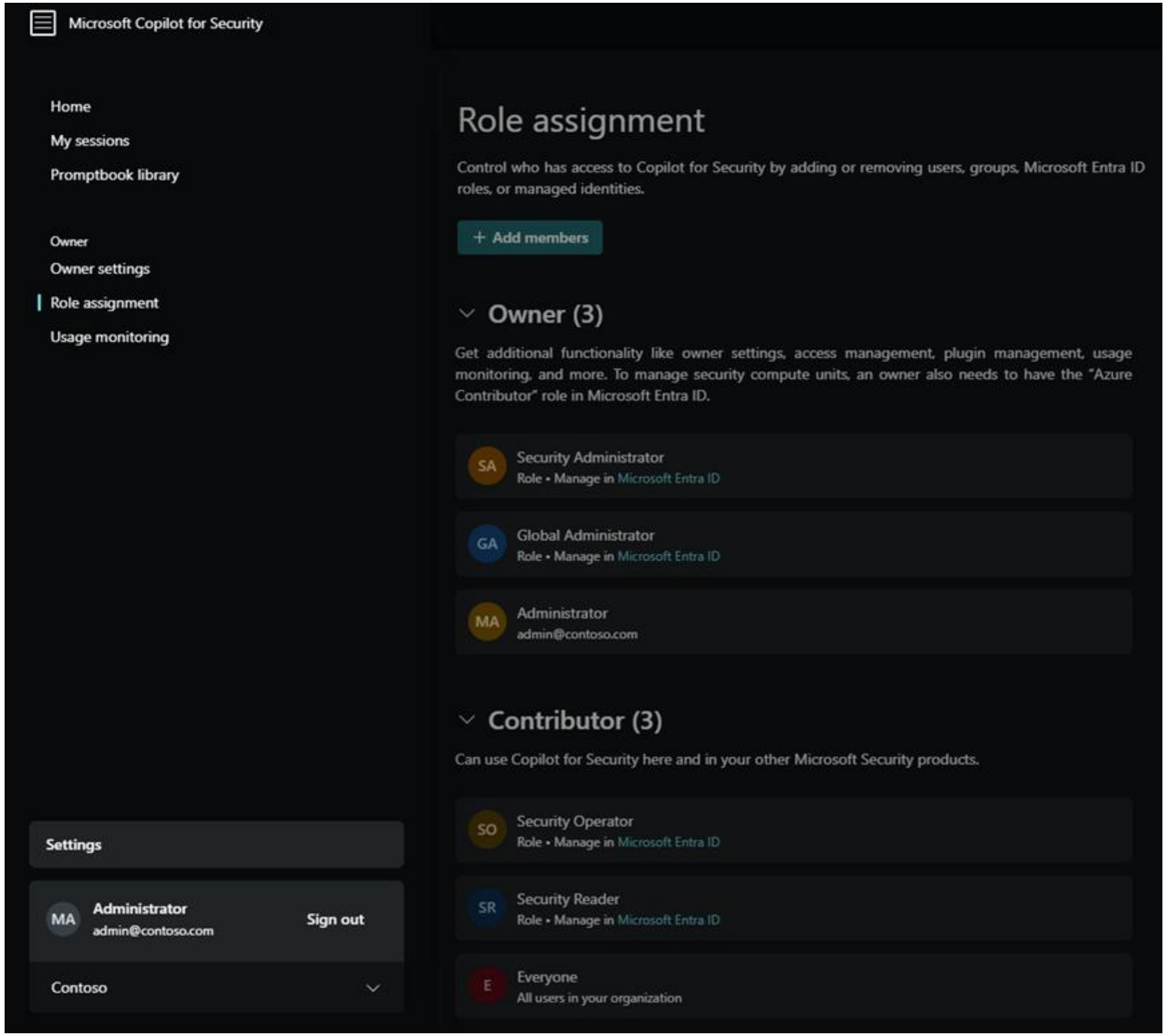
Turn on or create your own plugins to give Copilot access to the security services and websites you use. Learn more

**Microsoft** ⓘ ●

| | | |
|---|---|---|
| Azure AI Search (Preview)<br>Indexed data | | Set up |
| Microsoft Defender External Attack Surface Management<br>Attack surfaces, vulnerable assets, and attack surface insights | ⚙ | ○ |
| Microsoft Defender Threat Intelligence<br>Articles, intelligence profiles, vulnerabilities, indicators of compromise, hosts, and threat analytics | | ● |
| Microsoft Defender XDR<br>Alerts and incidents | | ● |

# Manage plugins

# Assign Copilot for Security access



Role assignment

Control who has access to Copilot for Security by adding or removing users, groups, Microsoft Entra ID roles, or managed identities.

Owner (3)

Get additional functionality like owner settings, access management, plugin management, usage monitoring, and more. To manage security compute units, an owner also needs to have the "Azure Contributor" role in Microsoft Entra ID.

SA Security Administrator
Role • Manage in Microsoft Entra ID

GA Global Administrator
Role • Manage in Microsoft Entra ID

MA Administrator
admin@contoso.com

Contributor (3)

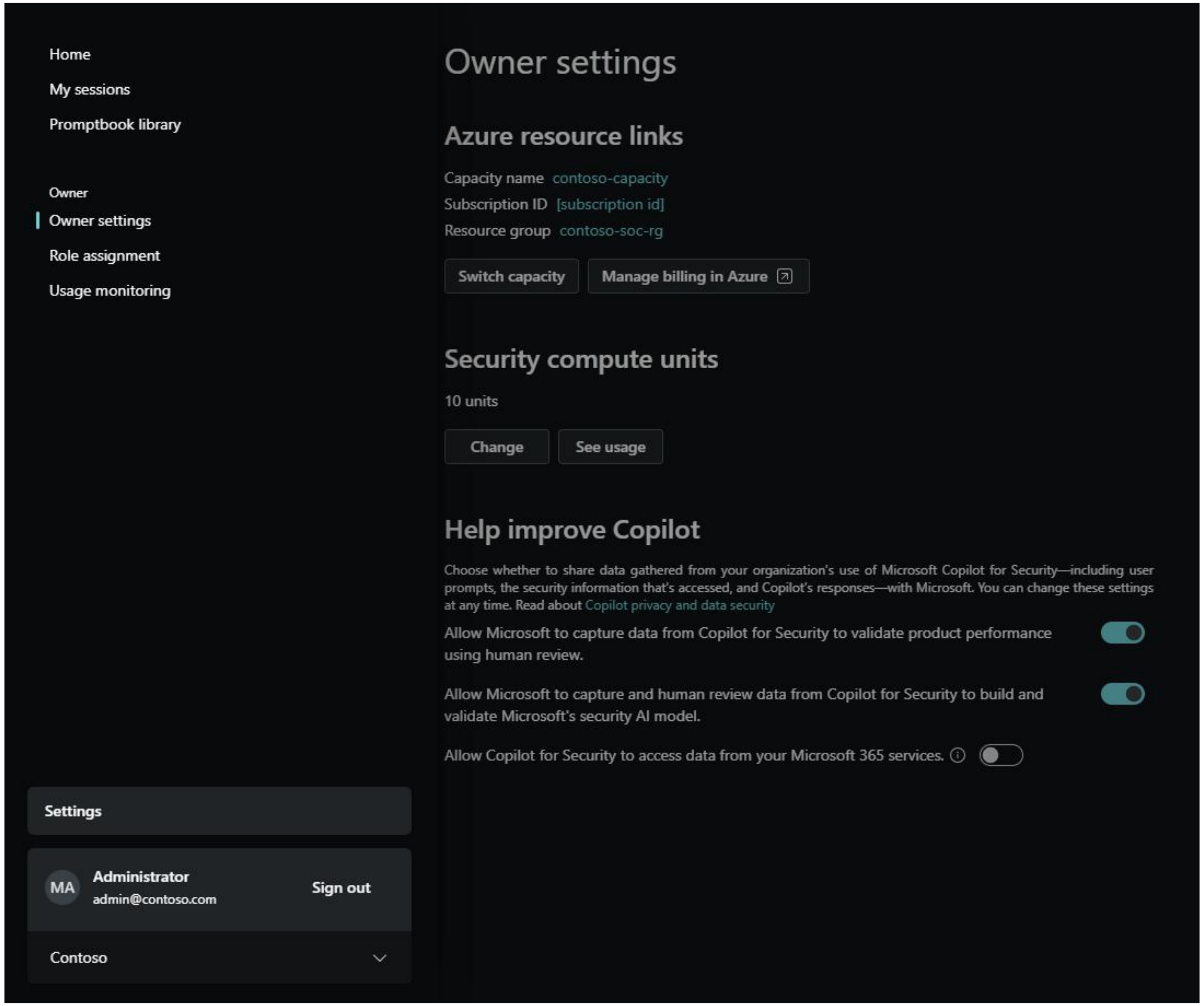
Can use Copilot for Security here and in your other Microsoft Security products.

SO Security Operator
Role • Manage in Microsoft Entra ID

SR Security Reader
Role • Manage in Microsoft Entra ID

E Everyone
All users in your organization

# Configure Owner settings



## Owner settings

### Azure resource links

Capacity name contoso-capacity
Subscription ID [subscription id]
Resource group contoso-soc-rg

### Security compute units

10 units

### Help improve Copilot

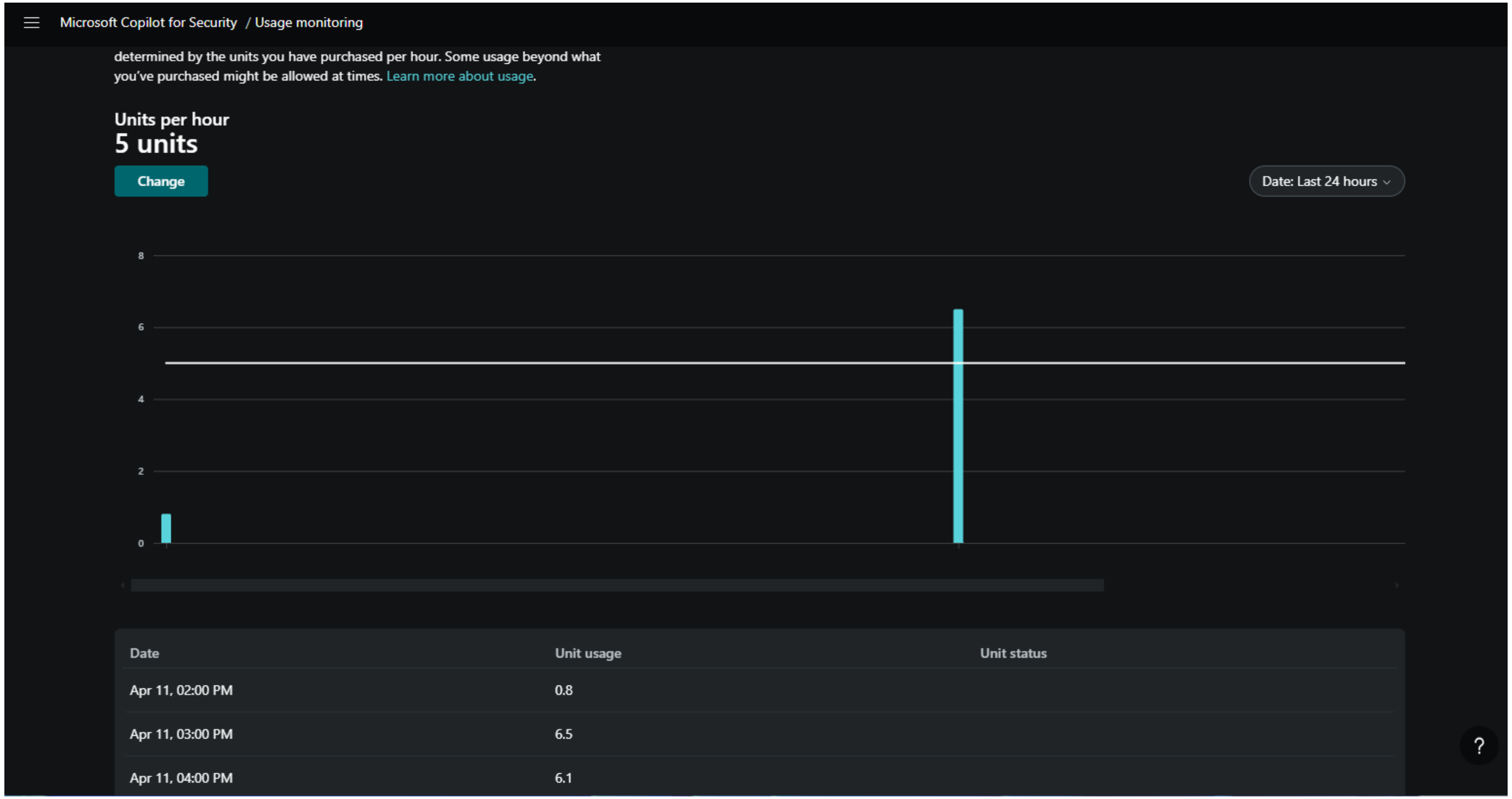
Choose whether to share data gathered from your organization's use of Microsoft Copilot for Security—including user prompts, the security information that's accessed, and Copilot's responses—with Microsoft. You can change these settings at any time. Read about Copilot privacy and data security

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. ●

Allow Copilot for Security to access data from your Microsoft 365 services. ⓘ ○

# Capacity management



determined by the units you have purchased per hour. Some usage beyond what you've purchased might be allowed at times. Learn more about usage.

Units per hour

5 units

| Date | Unit usage | Unit status |
|---|---|---|
| Apr 11, 02:00 PM | 0.8 | |
| Apr 11, 03:00 PM | 6.5 | |
| Apr 11, 04:00 PM | 6.1 | |

# Copilot for Security primary use cases

### Incident summarization

Gain context for incidents and improve communication across your organization by leveraging generative AI to swiftly distill complex security alerts into concise, actionable summaries, which then enable quicker response times and streamlined decision-making.

### Impact analysis

Utilize AI-driven analytics to assess the potential impact of security incidents, offering insights into affected systems and data to prioritize response efforts effectively.

### Reverse engineering of scripts

Eliminate the need to manually reverse engineer malware and enable every analyst to understand the actions executed by attackers. Analyze complex command line scripts and translate them into natural language with clear explanations of actions. Efficiently extract and link indicators found in the script to their respective entities in your environment.

### Guided response

Receive actionable step-by-step guidance for incident response, including directions for triage, investigation, containment, and remediation. Relevant deep links to recommended actions allow for quicker response.

# Copilot for Security integrations

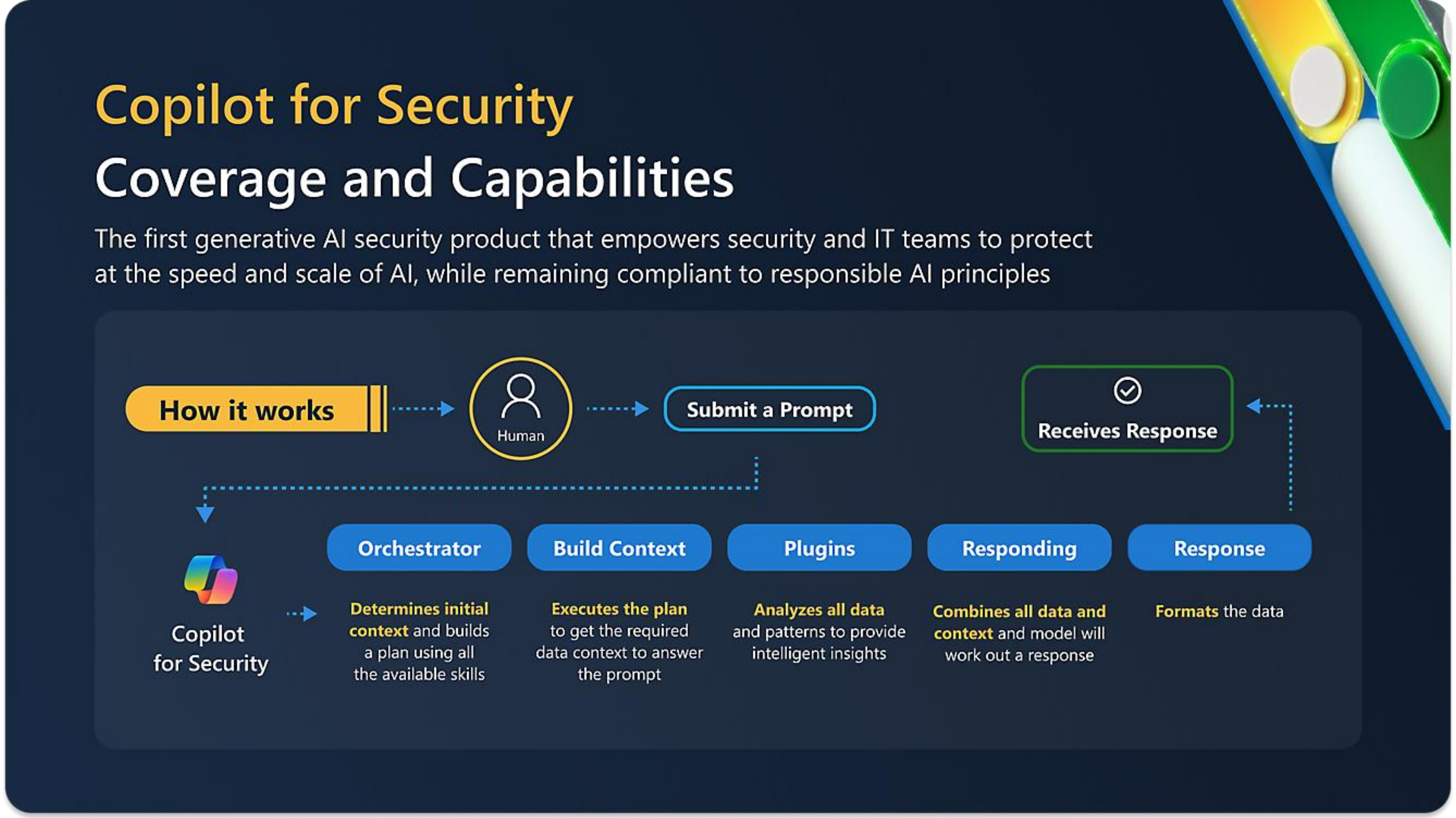
Copilot for Security integrates with products such as:

- Microsoft Defender XDR

- Microsoft Sentinel

- Microsoft Intune

- and other third-party services such as ServiceNow.



Copilot for Security

Coverage and Capabilities

The first generative AI security product that empowers security and IT teams to protect at the speed and scale of AI, while remaining compliant to responsible AI principles

How it works → Human → Submit a Prompt

Copilot for Security →

Orchestrator: **Determines initial context** and builds a plan using all the available skills

Build Context: **Executes the plan** to get the required data context to answer the prompt

Plugins: **Analyzes all data** and patterns to provide intelligent insights

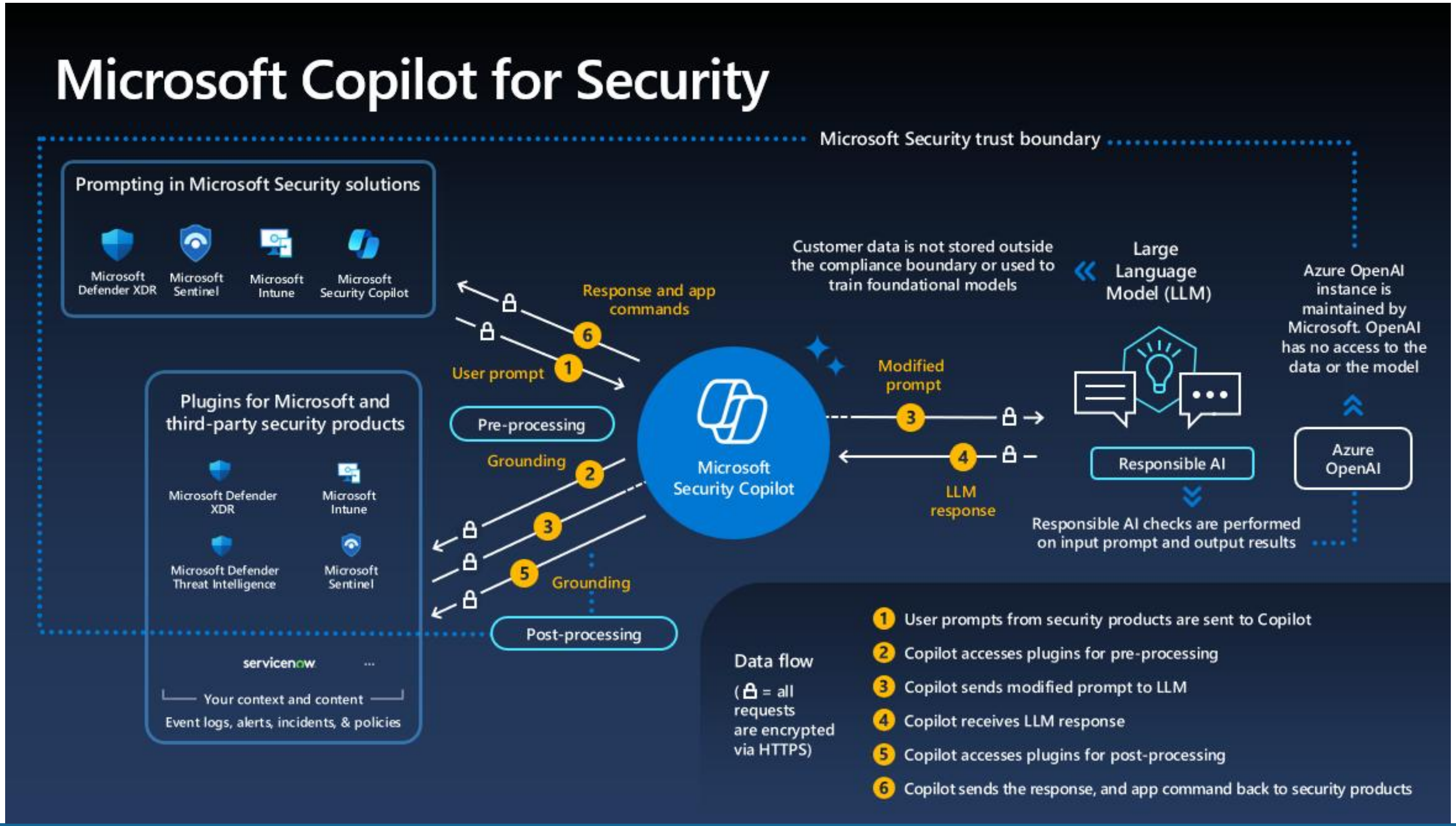
Responding: **Combines all data and context** and model will work out a response

Response: **Formats** the data

Receives Response

# How does Copilot for Security work

Microsoft Copilot for Security capabilities can be accessed through an immersive standalone experience and through intuitive embedded experiences available in other Microsoft security products.



## Microsoft Copilot for Security

Microsoft Security trust boundary
Prompting in Microsoft Security solutions
Microsoft Defender XDR
Microsoft Sentinel
Microsoft Intune
Microsoft Security Copilot
Response and app commands
6
User prompt
1
Plugins for Microsoft and third-party security products
Microsoft Defender XDR
Microsoft Intune
Microsoft Defender Threat Intelligence
Microsoft Sentinel
servicenow
...
Your context and content
Event logs, alerts, incidents, & policies
Pre-processing
Grounding
2
3
5
Grounding
Post-processing
Microsoft Security Copilot
Customer data is not stored outside the compliance boundary or used to train foundational models
Modified prompt
3
4
LLM response
Large Language Model (LLM)
Responsible AI
Responsible AI checks are performed on input prompt and output results
Azure OpenAI instance is maintained by Microsoft. OpenAI has no access to the data or the model
Azure OpenAI

Data flow

(🔒 = all requests are encrypted via HTTPS)

1. User prompts from security products are sent to Copilot
2. Copilot accesses plugins for pre-processing
3. Copilot sends modified prompt to LLM
4. Copilot receives LLM response
5. Copilot accesses plugins for post-processing
6. Copilot sends the response, and app command back to security products

# How does Copilot for Security work

Microsoft Copilot for Security capabilities can be accessed through an immersive standalone experience and through intuitive embedded experiences available in other Microsoft security products.

# Pricing

## Microsoft Copilot for Security compute capacity

Provision capacity in Security Compute Units (SCU) to run Copilot for Security workloads.

These workloads provide insights, evaluate prompts, run promptbooks and automate them in both the standalone product and embedded experiences across Microsoft Security.

Flexibly provision compute units to meet your organization needs.

| SKU | Price per hour | Estimated price per month |
|---|---|---|
| Provisioned | $4 | $2,920[1] |

# Tops for prompting

- Be clear and precise.
- Give  a lot of context.
- Tell if the format you need.
- Give it sources to relevant info.
- Address it directly as „you”.

# Demo

KEEP
CALM
AND
PRAY THE DEMO
WORKS

KEEP
CALM
AND
PRAY THE DEMO
WORKS

I am actively seeking new opportunities and exciting challenges. If you would like to get in touch, please feel free to reach out through the following channels:

zalnet
BEATA ZALEWA

Email: beata@zalnet.pl

LinkedIn: https://www.linkedin.com/in/beatazalewa/

Blog: https://zalnet.pl/blog/

X: https://x.com/beatazalewa

GitHub: https://github.com/beatazalewa/Conferences/