Microsoft Copilot for Security – the good, the bad and the ugly

Beata Zalewa, BSides 2024, 14.07.2024

zalnet

About me

Security Architect

Consultant

Microsoft Certified Trainer

AI & Cybersecurity Practitioner

Developer

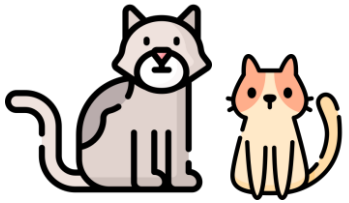
Freelancer

Azure @ ❤

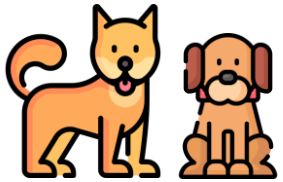
Google Cloud

1 Husband

1 Daughter



2 cats



2 dogs

Detective stories

Photography

zalnet BEATA ZALEWA

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

beata@zalnet.pl

BLOG 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.

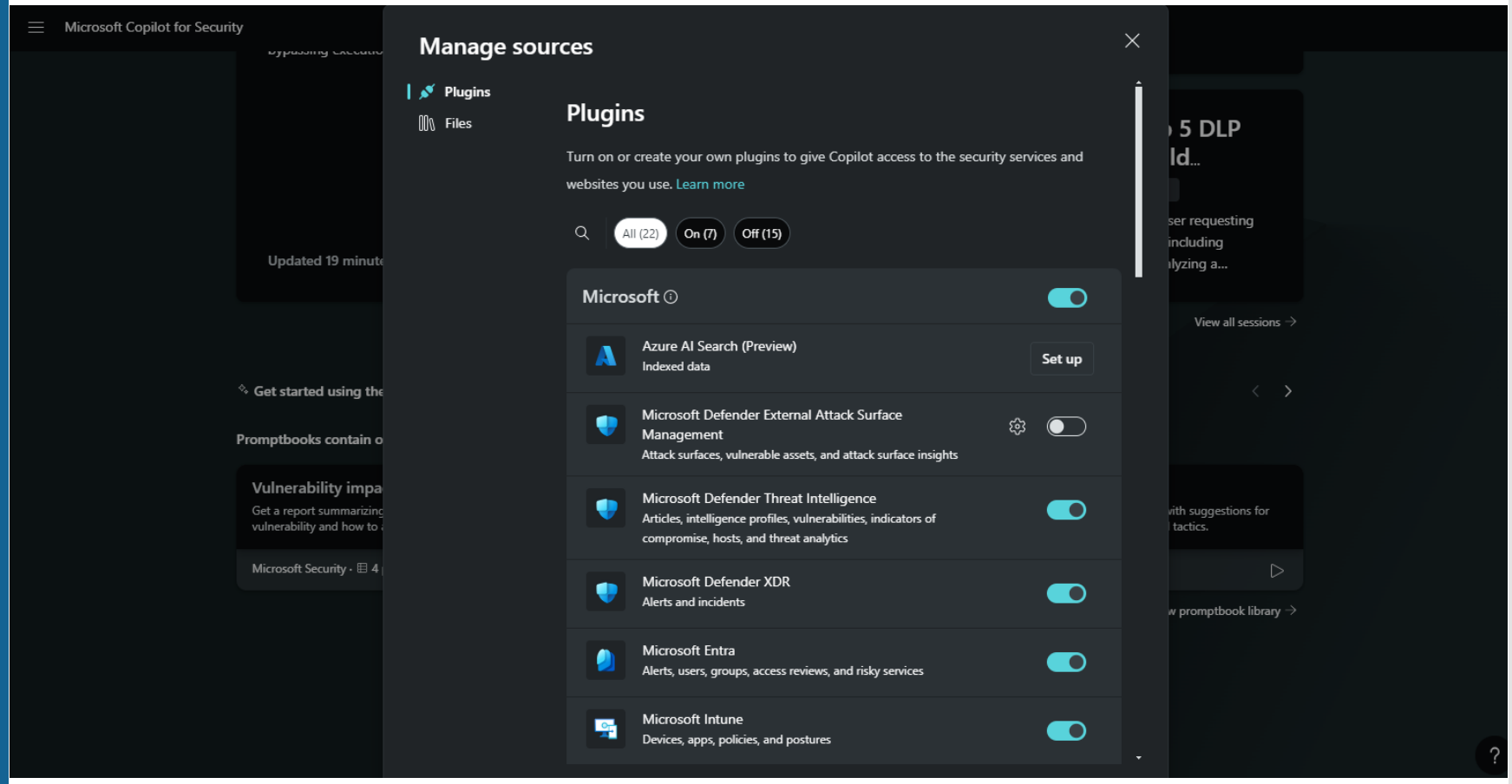
zalnet

Copilot for Security and OpenAI

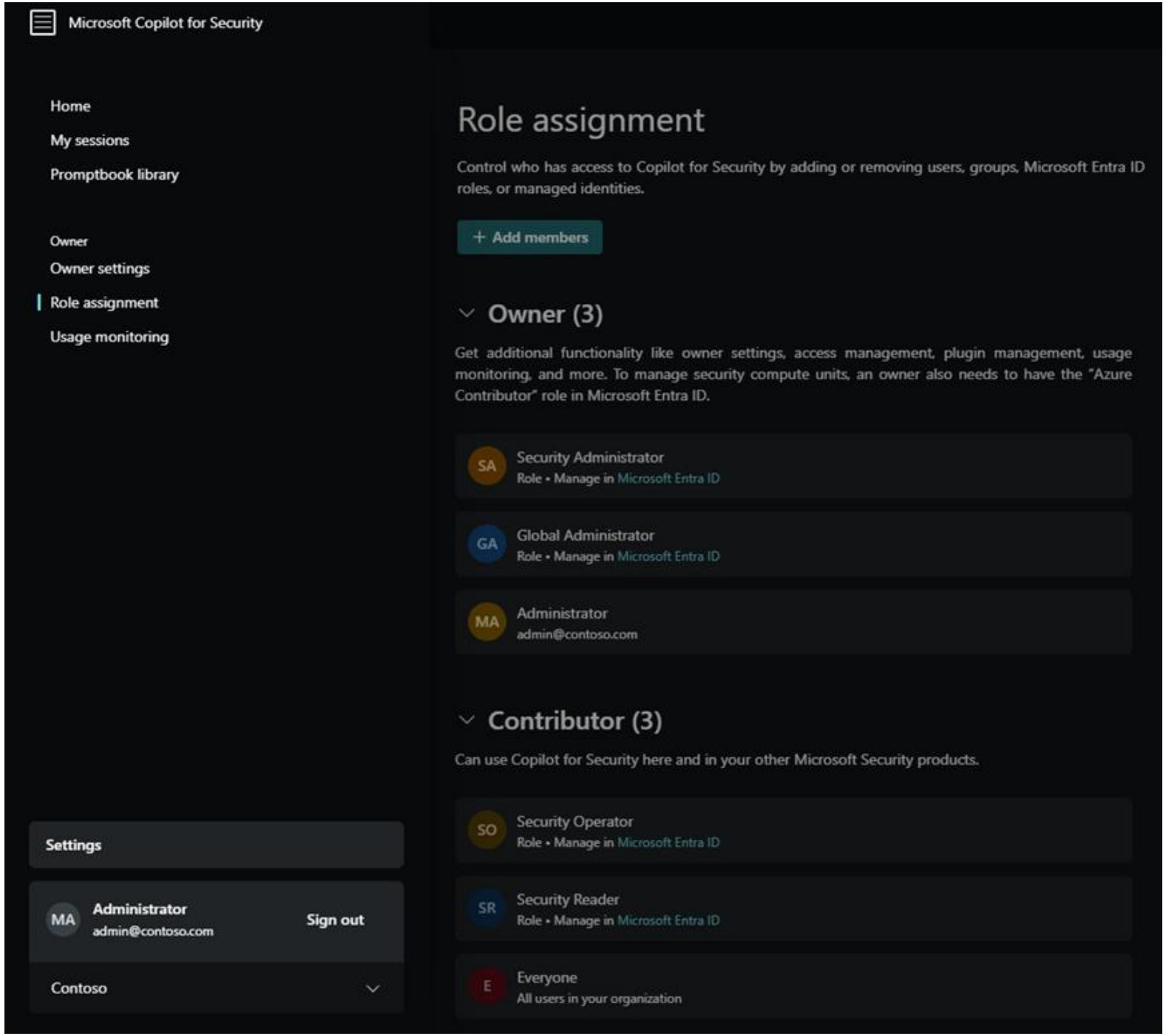
The solution leverages the full power of **OpenAI** architecture to generate a response to a user prompt by using security-specific plugins, including organization-specific information, authoritative sources, and global threat intelligence.

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.

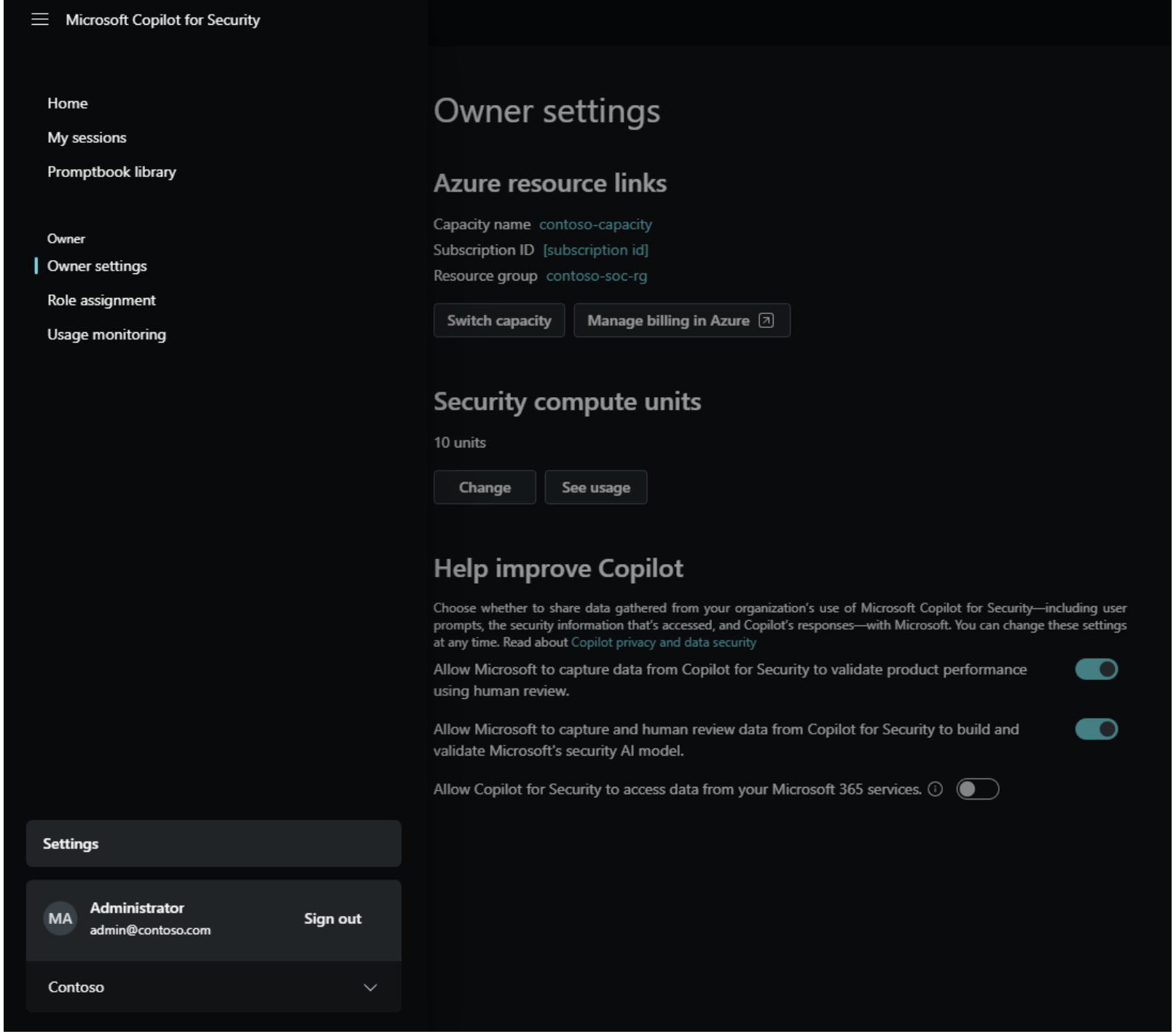
Manage plugins



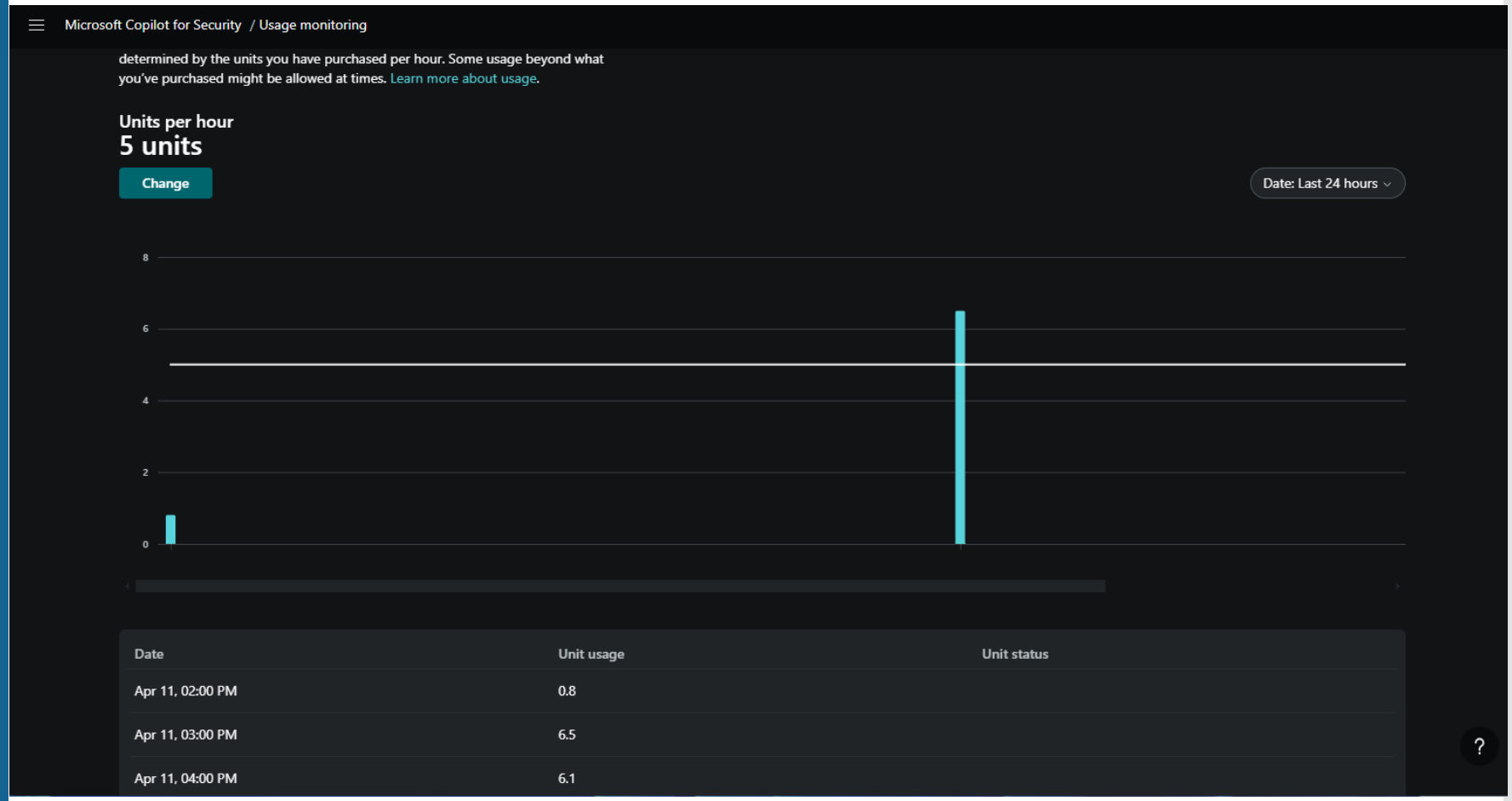
Assign Copilot for Security access



Configure Owner settings



Capacity management



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.

zalnet

Copilot for Security integrations

Copilot for Security integrates with products such as:

Microsoft Defender XDR

Microsoft Sentinel

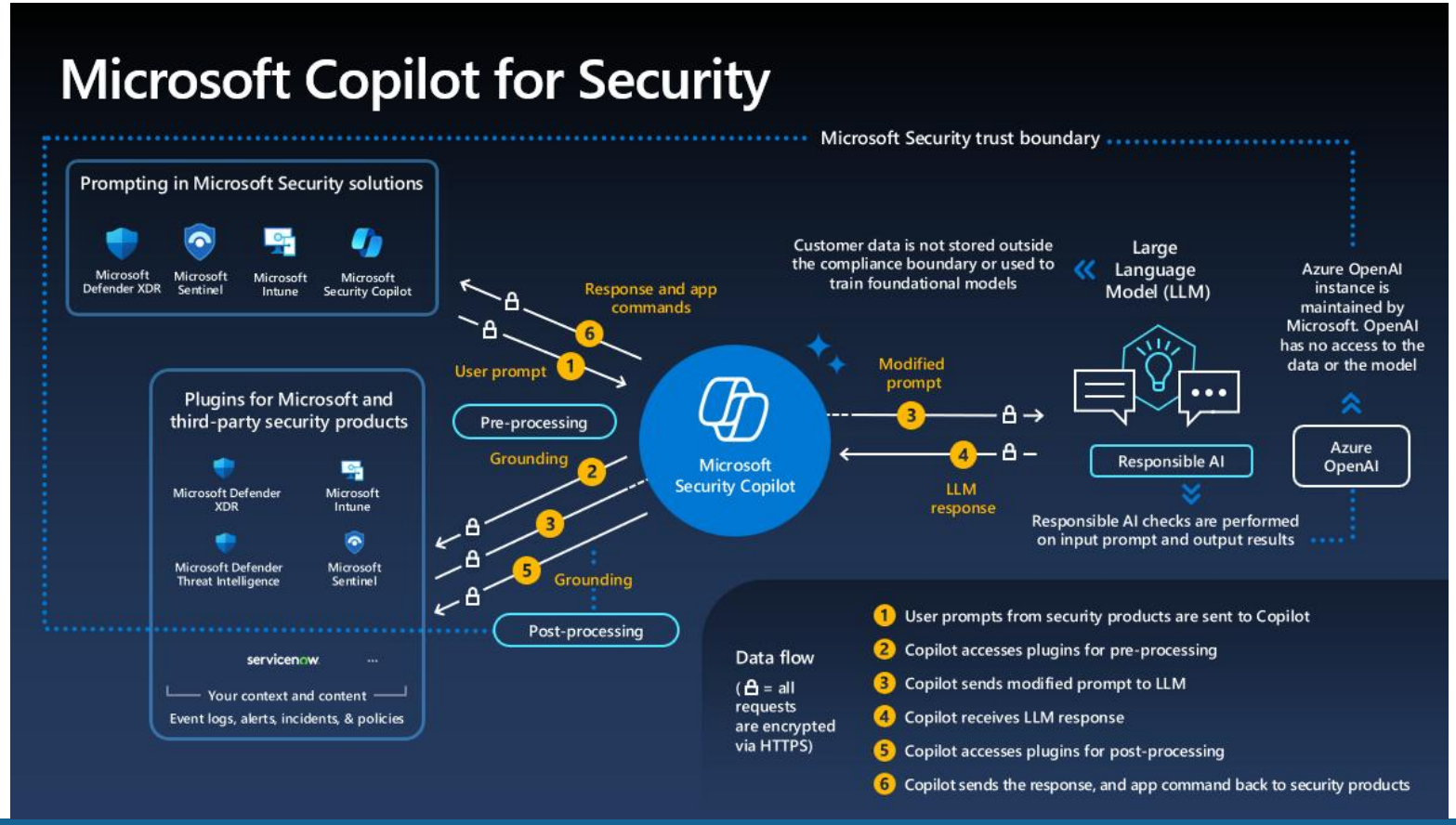
Microsoft Intune

and other third-party services such as ServiceNow.

zalnet

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.



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	$2,880[1]

Tips 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”.

Used resources

https://github.com/Azure/Copilot-For-Security

https://thecfsprompt.substack.com/p/the-prompt-for-copilot-for-security-10a

LinkedIn's group: Copilot for Security

https://www.linkedin.com/groups/14345161/

zalnet

Demo

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/