



Bringing AI to Security with Microsoft Copilot for Security

Global Azure - Bergen - 18. April 2024 - Jan Vidar Elven

Azure
User group
Norway



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**.

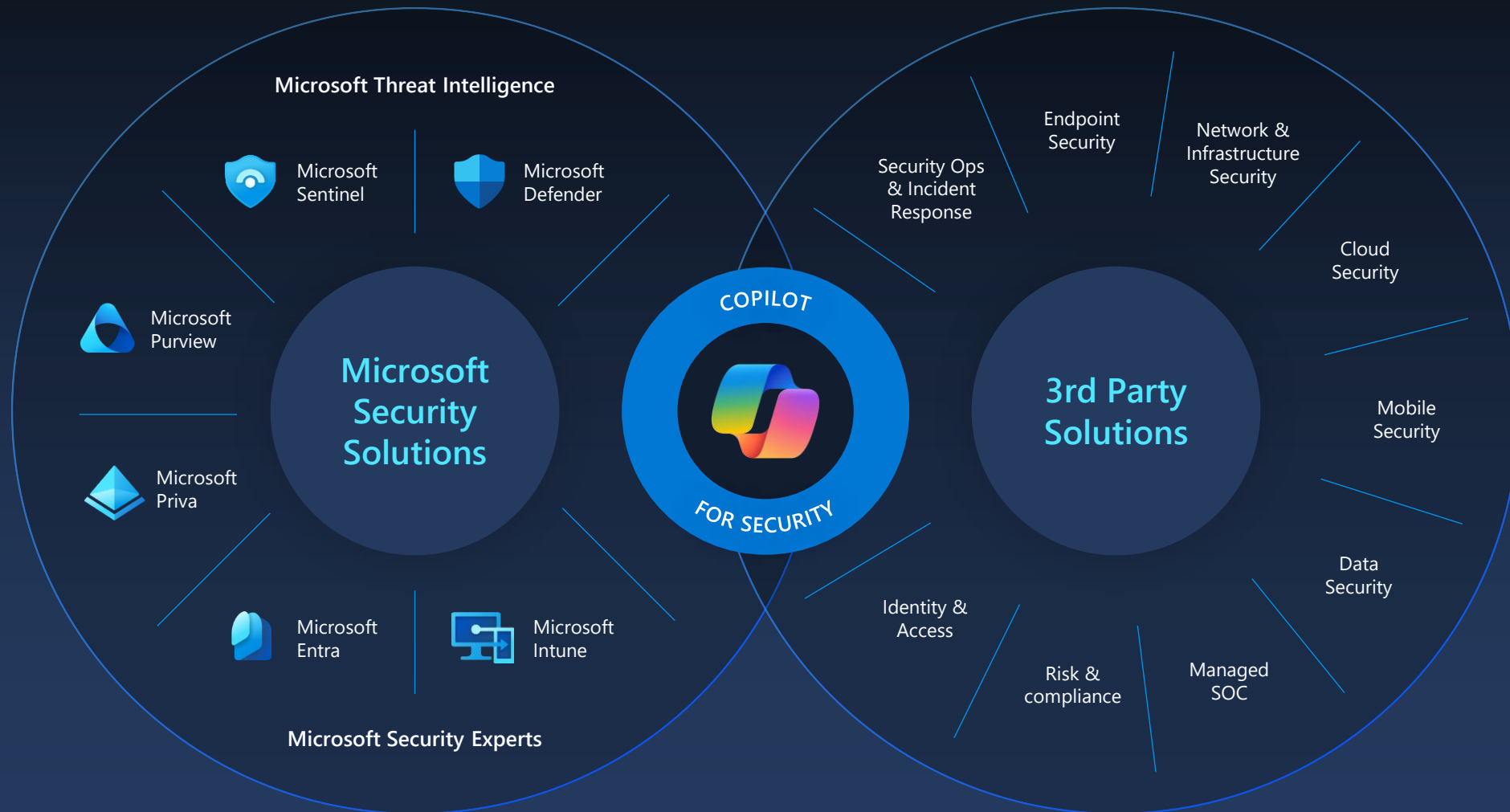
Some include:

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

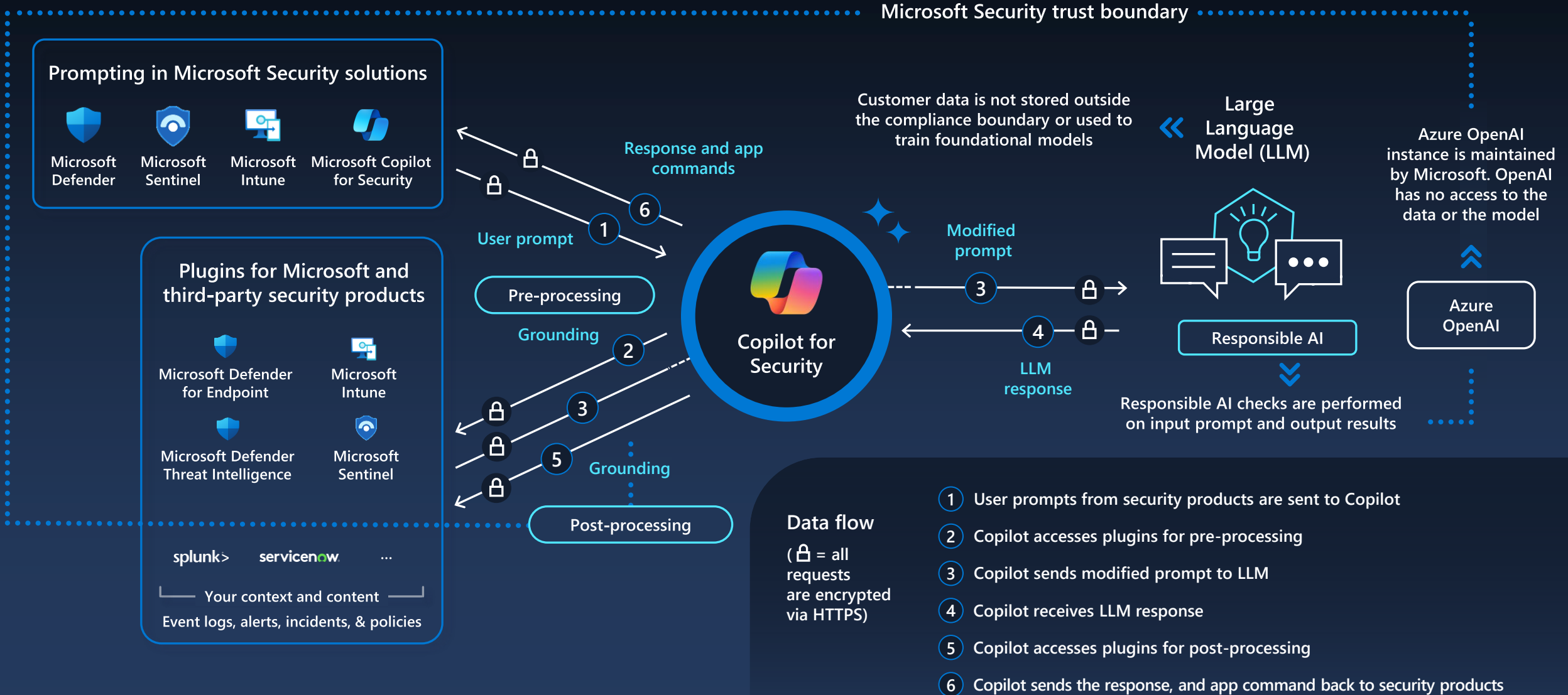


The Copilot for Security advantage


Copilot stitches together information across all security products



Architecture – data flow for Copilot for Security



Copilot for Security standalone experience

 Microsoft Security Copilot Preview

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...

[View all sessions →](#)


Explore with Copilot


 Featured prompts

 Promptbooks

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






 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



Copilot for Security embedded experience

- Microsoft Entra
- Microsoft Intune
- Microsoft Defender XDR
- Microsoft Purview
- Microsoft Defender Threat Intelligence



Welcome to Microsoft Copilot for Security

Let's get your organization set up.

Get started



Setting up your tenant ...

This might take a couple of minutes.

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 ⓘ

Microsoft Azure Sponsorship



Resource group ⓘ

(new) rg-sec-copilot-scu-we



[Create a new one](#)

Capacity name ⓘ

scu-elven-we

Prompt evaluation location ⓘ

Europe



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

Capacity region ⓘ

Europe West

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](#)



Setting up your security capacity ...

This might take a couple of minutes.



Your Customer Data will be stored in Europe

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

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

Back

Continue



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](#)

Back

Continue



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](#)

Back

Continue



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	scu-elven-we
Subscription	b1193530-4663-4bc7-90de-1d0d44576ba7
Resource group	rg-sec-copilot-scu-we
Location	Europe West

Share this link with your security colleagues:

[securitycopilot.microsoft.com](#)

[Manage billing in Azure portal](#)

[Back](#)

[Finish](#)



DEMO



Technical Skilling Curriculum



1

Beginner



2

Intermediate



3

Advanced



Part 1: Getting Started

- ☐ Module 0: Other Learning and Support Options
- ☐ Module 1: Introduction and Onboarding
- ☐ Module 2: Configuration
 - ☐ Understanding Authentication
 - ☐ Introduction to Plugins
 - ☐ Prompting in Microsoft Copilot for Security
- ☐ Module 3: Features and Overview
 - ☐ Understanding Architecture
 - ☐ Standalone Experience
 - ☐ Embedded Experience
 - ☐ Plugins
 - ☐ Prompting and Promptbooks
 - ☐ Get Started with Use Cases
- ☐ Bonus Module: Understanding the Basics of Generative AI and Prompt Engineering

Part 2: Become Proficient

- ☐ Module 1: Microsoft Security Product Plugins
 - ☐ Microsoft Defender XDR
 - ☐ Microsoft Entra
 - ☐ Microsoft Intune
 - ☐ Microsoft Defender Threat Intelligence and Threat Analytics
 - ☐ Microsoft Purview
 - ☐ Microsoft Defender External Attack Surface Management
- ☐ Module 2: OpenAI Copilot for Security Plugins
 - ☐ Generic
 - ☐ Public Web
- ☐ Module 3: Creating Effective Prompts
- ☐ Module 4: Managing Plugins
- ☐ Module 5: Third-Party Plugins

Part 3: Grow into an Expert

- ☐ Module 1: Custom Promptbooks
- ☐ Module 2: Custom Plugins
- ☐ Module 3: Automation Scenarios for Microsoft Copilot for Security using Logic Apps
- ☐ Module 4: Connect your Knowledge Base to Microsoft Copilot for Security



[How to Become a Microsoft Copilot for Security Ninja: The Complete Level 400 Training](#)



Certificate of Completion

THIS IS TO ACKNOWLEDGE THAT

Jan Vidar Elven

HAS SUCCESSFULLY COMPLETED ALL THE REQUIREMENTS FOR
Microsoft Copilot for Security Ninja Training



4/17/2024

Copilot Team
SIGNED, Copilot for Security Team

