

Microsoft Security Copilot



A large, irregularly shaped collage of various characters and weapons. At the top center is a character with a wide, toothy grin and a single eye. To its right is a character with a large, open mouth showing sharp teeth. Below these are several other characters, some with mechanical or cybernetic features, and various weapons like knives, swords, and firearms. The entire collage is rendered in a high-contrast, black and white style with yellow highlights.

**WE HAVE THE
ANGRIEST
END USERS**



Not Bad
Security

**Briefly on the
landscape of
AI and
security**

**Custom
solutions**

**Security
Copilot**

**Stuff I forgot
and might
mention later**



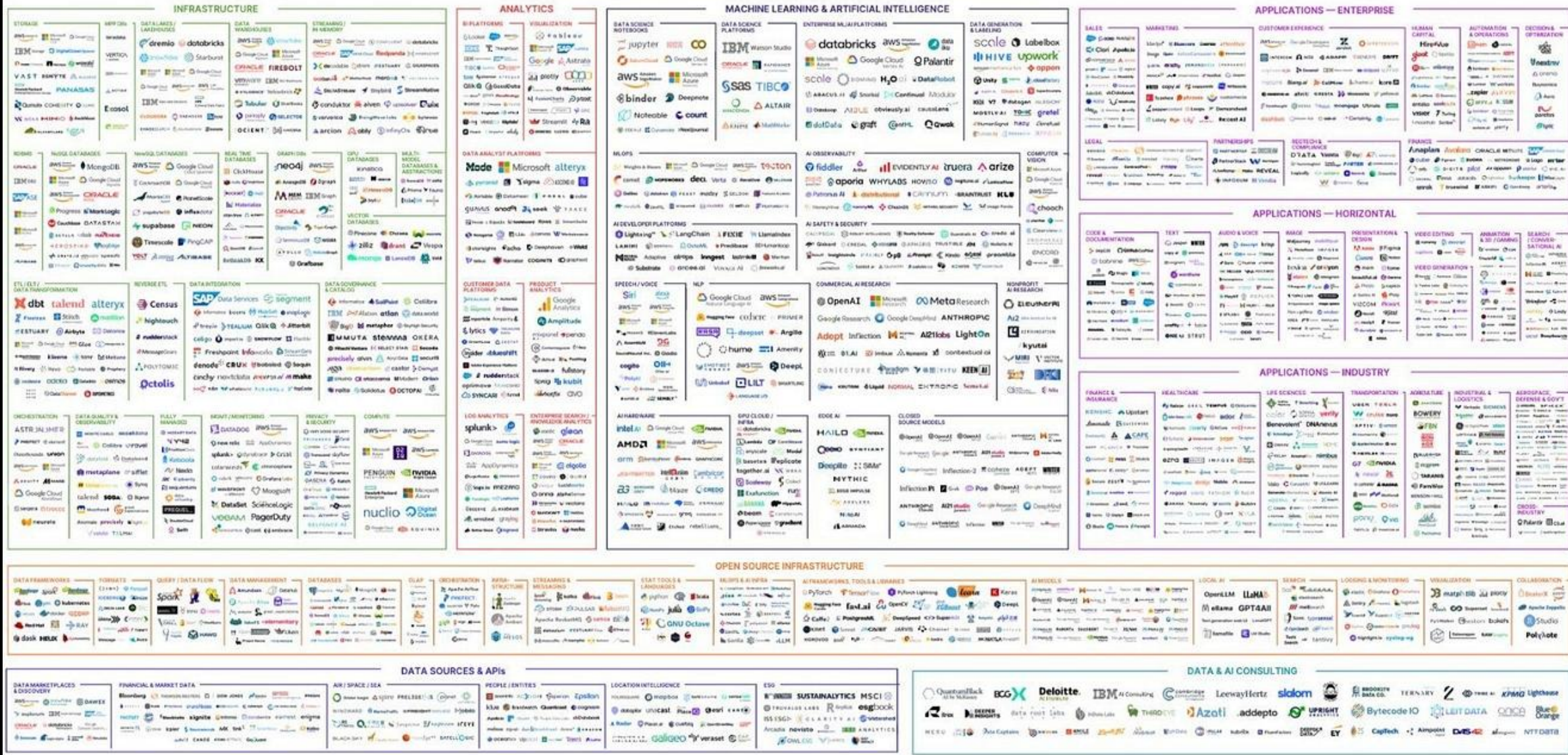
| There have been two major developments in the past two years.



Skibidi toilet

The landscape of AI

THE 2024 MAD (MACHINE LEARNING, ARTIFICIAL INTELLIGENCE & DATA) LANDSCAPE



| Large (and Small) Language Models



HUGGING FACE

1,463,175



Phi-4



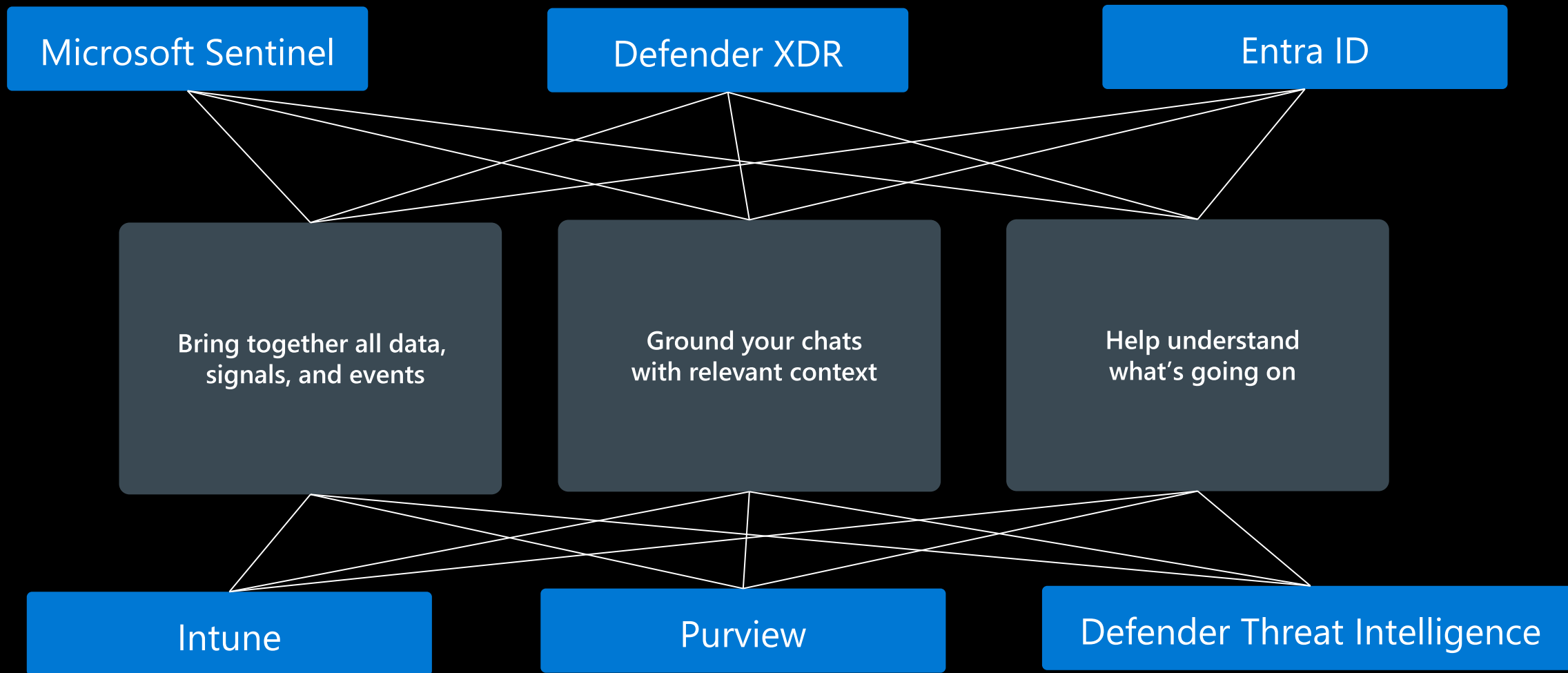
Microsoft Copilot  @MSFTCopilot

Ad ...

Track discussions in real time and produce conversation summaries with Copilot for Microsoft 365 and Teams.



Security Copilot: Microsoft's AI approach to security



Standalone vs. Embedded

Continue your last session

Give me all the details and possible risks associated with...

User Account Potential Risks Account Details +2

The conversation revolves around the details and potential risks associated with the user account jussimvp@jussimvp.onmicrosoft.com. The user, Jussi Roine, has an active account with various personal details

Updated 14 minutes ago

Azure Copilot Session - a5149c6e-...

Summarization isn't possible as there are no prompts in this session.

Microsoft Sentinel incident investigation

Sentinel Incident 1 +3

The conversation revolves around the investigation of Sentinel Incident 1, which is a high severity incident with the title 'OMG...

View all sessions →

Get started using these promptbooks

Promptbooks contain one or more prompts that run in sequence automatically. [Learn more](#)

Microsoft Sentinel incident invest...

Get a report about a specific incident, along with related alerts, reputation scores, users, and...

Microsoft Security · 7 prompts

Threat actor profile

Get a report profiling a known actor with suggestions for protecting against common...

Microsoft Security · 5 prompts

Vulnerability impact assessment

Get a report summarizing the intelligence for a known vulnerability and how to address it.

Microsoft Security · 4 prompts

View promptbook library →

🔍 📄 ▶

Microsoft Entra admin cent...

Search resources, services, and docs (G+/)

jussimvp@jussimvp
CAPE BERRY (JUSSIMVP.ON)

- Home
- Diagnose & solve problems
- Favorites
- Identity
- Overview
- Users

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

Tell me about Intune setting "App lists"

user. Try another user or share your feedback.

The Intune setting "App lists" is part of the "MacEndpointProtection" policy type for macOS under the "Firewall" category. This setting allows you to specify apps and rules for incoming connections for the app.

There are two local setting definitions related to "App lists":

- The first setting allows you to select apps that are explicitly allowed to receive incoming connections. This setting is not required.
- The second setting allows you to select apps that should block incoming connections. This setting is also not required.

Here's how you can configure the "App lists" setting:

- Expand the dropdown and then select **Add** to specify apps and rules for incoming connections for the app.
- Allow incoming connections**
 - Not configured
 - Block
 - Allow
- Bundle ID** - The ID identifies the app. For example: `com.apple.app`

This setting is part of the macOS firewall profile in the Endpoint Security policy for macOS Firewalls.

Please note that the setting ID "MacEndpointProtection_Firewall_macFirewallTableName_4910" is specific to the internal system and may not be directly visible or editable.

Sources:
[1]: [Firewall policy settings for endpoint security in Intune](#)

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

Embedded for Incident Management

Lateral movement incident

High

Active

Unassigned

Attack story

Alerts (2)

Assets (1)

Investigations (0)

Evidence and Response (5)

Summary

Similar incidents (5)

Alerts

Play attack story

Unpin all

Show all

May 13, 2024 11:37 AM

New

[SAMPLE ALERT] Malicious file uploaded to storage account

Sample-Storage

May 13, 2024 11:38 AM

New

[SAMPLE ALERT] Potential malware uploaded to a storage file share

Sample-Storage

Incident graph

Layout

Group similar nodes

Sample-Name

00.00.00.00

2 Files

Sample-Storage

Sample-Name

Incident details

Assigned to

Unassigned

Classification

Not set

First activity

May 13, 2024 11:37:06 AM

Incident ID

16

Categories

Lateral movement

Last activity

May 13, 2024 11:38:02 AM

Impacted assets

Cloud Resources (1)

Sample-Storage

Resource Type

Storage Account

Active alerts in this incident (2/2)

High (2)

Medium (0)

2 more

View all alerts

Incident summary

May 15, 2024 2:01 PM

The high severity incident 'Lateral movement incident' occurred between 2024-05-13 08:37:06 UTC and 2024-05-13 08:38:02 UTC.

LateralMovement: At 2024-05-13 08:37:06 UTC, a malicious file named 'Sample-Name' was uploaded to a storage account. This action is indicative of an attempt at lateral movement within the network.

LateralMovement: Shortly after, at 2024-05-13 08:38:02 UTC, potential malware was uploaded to a storage file share. The file, also named 'Sample-Name', was associated with the IP address 00.00.00.00 (US - United States). This further suggests lateral movement and potential compromise of the network.

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

Guided response

Identifying response actions...

Stop generating

Prompts

We need to get better with prompt engineering

How can Copilot for Security help?



GENERIC

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.

Extract entities

Extract entities (e.g. accounts, URLs, hashes) from security data (e.g. logs, alerts and incidents)

Extract indicators of compromise

Extract indicators of compromise from plain text.

Generate security examples

Generate security-specific examples, such as event logs, reports, and configuration instructions.

Summarize data

Get a summary of the given data.

You don't have to be brief - explain and provide context

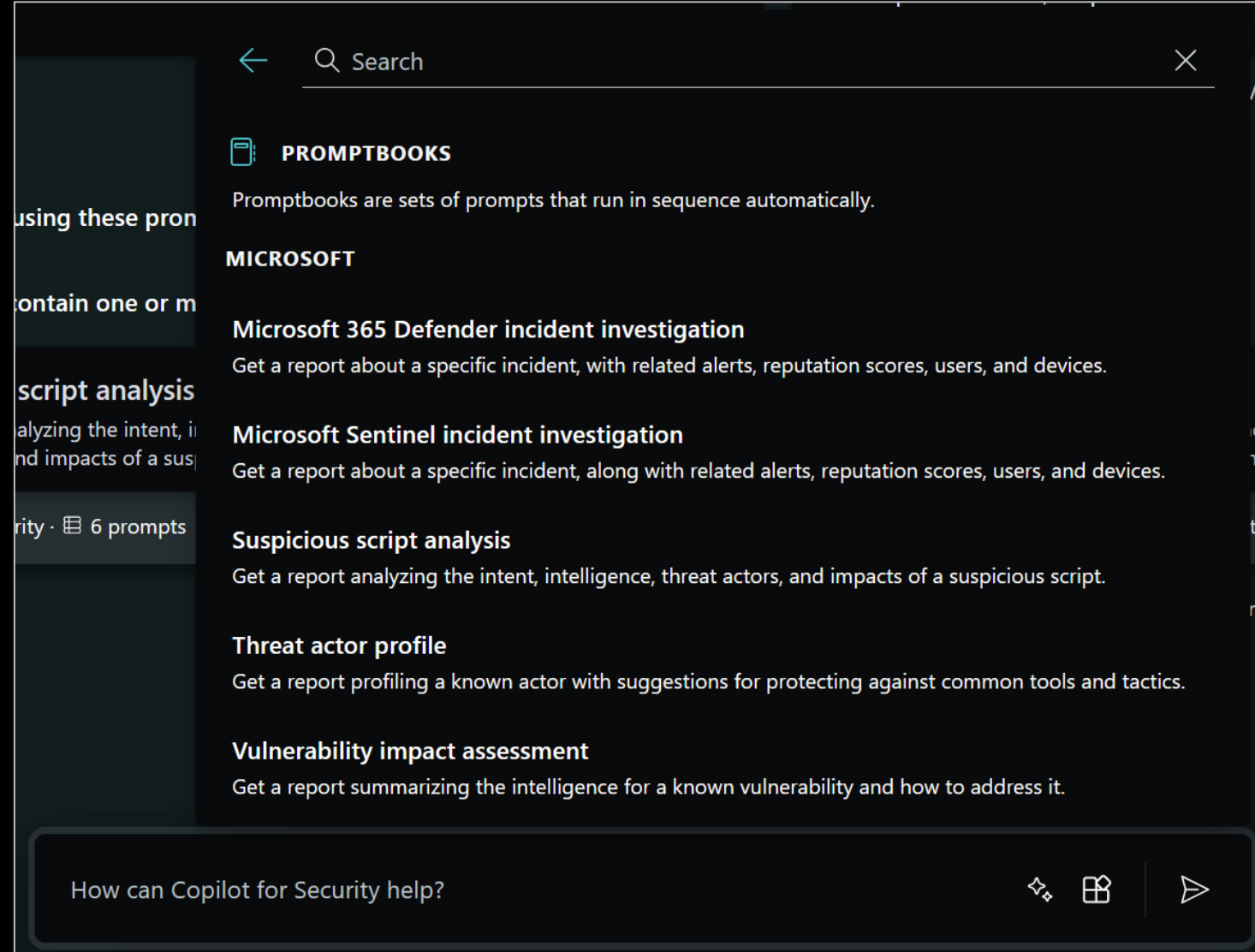
Similar rules as for ChatGPT / Azure OpenAI prompts, see [prompt engineering guidance](#)

| Promptbooks

SC includes a series of prebuilt prompts – known as Promptbooks

Think of them as built-in workflows

Custom promptbooks are easy to create



DEMO: Setup and basic use



| You lose about 1% of muscle mass per year, once you turn 50



Eat more broccoli!

| Interesting use cases

Generate KQL

Here is the KQL query that you requested:

```
1 DeviceInfo
2 | where OSPlatform in ("WindowsServer2012", "WindowsServer2012R2")
3 | where Region == "West Europe"
4
```

Create incident reports

Incident summary

The high severity incident 'Lateral movement incident' occurred between 2024-05-13 08:37:06 UTC and 2024-05-13 08:38:02 UTC.

- **LateralMovement:** At 2024-05-13 08:37:06 UTC, a malicious file named 'Sample-Name' was uploaded to a storage account. This action is indicative of an attempt at lateral movement within the network.

Classification

Incident is unclassified

Investigation actions

No investigation actions yet

Remediation actions

No remediation actions yet

Follow-up actions

No follow-up actions yet

Analyze files and scripts

🔍 Analyze a script or command

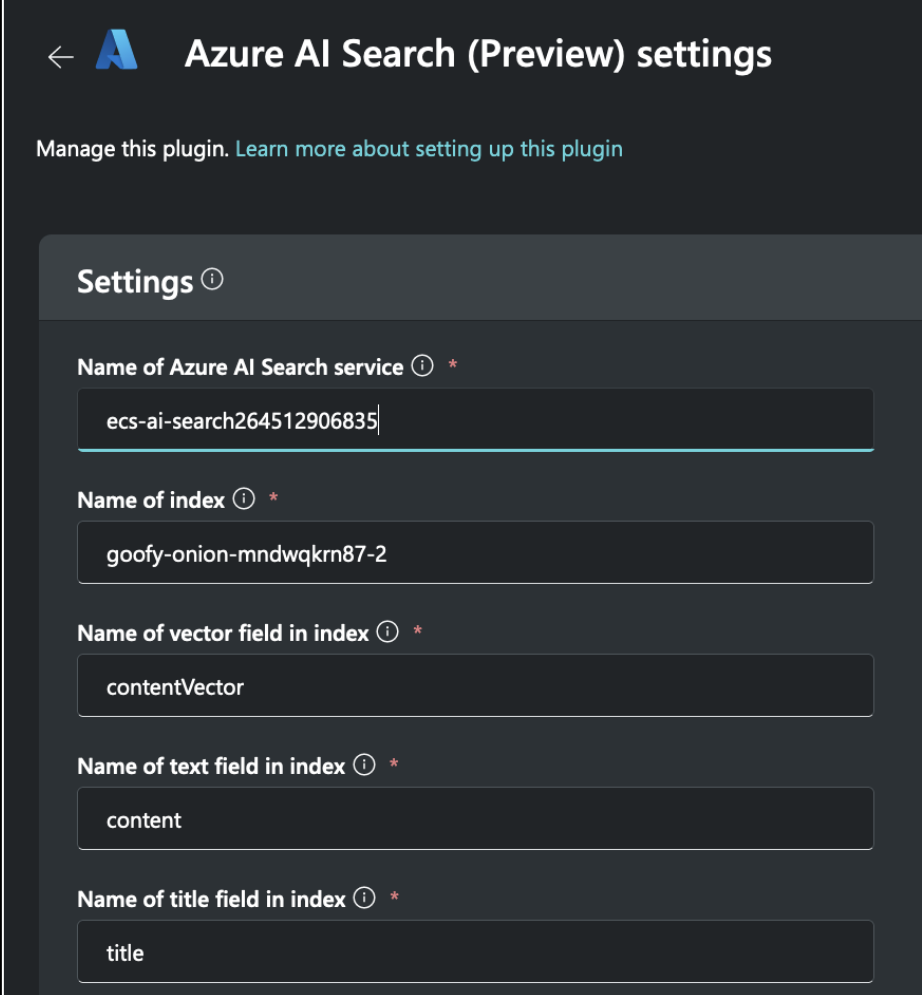
Script:#Source: <https://0x00-0x00.github.io/research/2018/11/06/Recovering-Plaintext-Domain-Credentials-From-WPA2-Enterprise-on-a-compromised-host.html> function Get-String { Param([Parameter(Mandatory = \$true, Position = 0)] [byte[]]\$InputStream) [byte[]]\$Output = @(); foreach(\$byte in \$InputStream) { if(\$byte -eq 0) { return \$Output } else { \$Output += \$byte } } } function Get-System { if([System.Threading.Thread]::CurrentThread.GetApartmentState() -ne 'STA') { Write-Output "This powershell shell is not in STA mode!"; return ; } if(-not ([System.Management.Automation.PSTypeName]"zc00l.ImpersonationToken").Type) {

| Organizational knowledge

GenAI lives and breathes from vectors

Azure AI Search plugin allows to pull in organizational data to enrich findings and solutions.

Azure AI Search must be populated with data – use Azure OpenAI Embeddings-model to generate it initially.



The screenshot shows the 'Azure AI Search (Preview) settings' page. At the top, there is a back arrow and the Azure logo. Below the title, a link says 'Manage this plugin. Learn more about setting up this plugin'. The main section is titled 'Settings' with an information icon. It contains five form fields, each with a label, an information icon, and a required field asterisk:

- Name of Azure AI Search service**: The input field contains 'ecs-ai-search264512906835'.
- Name of index**: The input field contains 'goofy-onion-mndwqkrn87-2'.
- Name of vector field in index**: The input field contains 'contentVector'.
- Name of text field in index**: The input field contains 'content'.
- Name of title field in index**: The input field contains 'title'.

Plugins



Copilot for Security plugin
Custom .yaml or .json



OpenAI plugin
manifest.json

Microsoft ⓘ

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

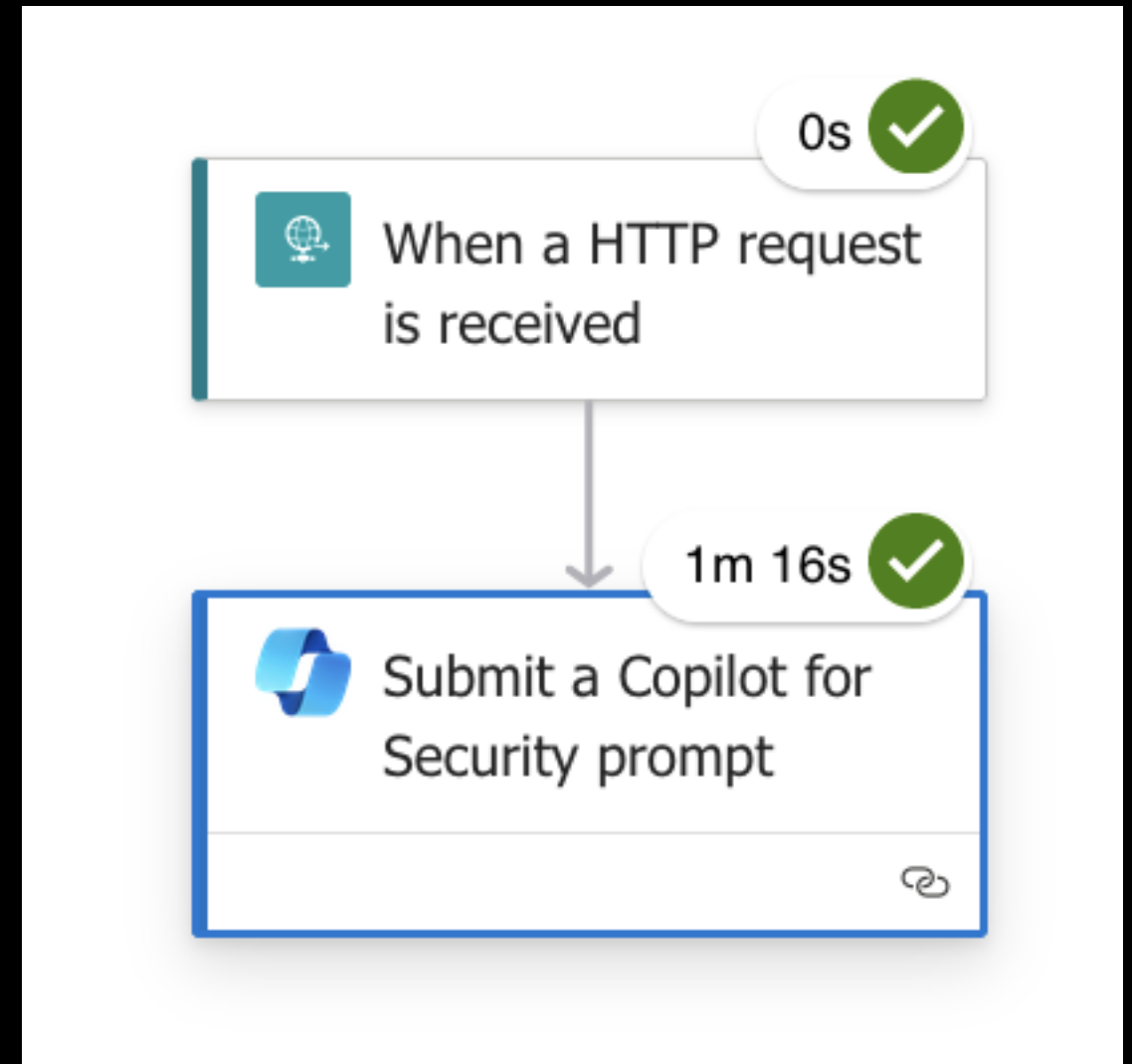
Show less ^

	CIRCL Hash Lookup (Preview) ⓘ File hashes	<input type="checkbox"/>
	Copilot for Security Plugin for ServiceNow (Preview) ⓘ Cases	Set up
	Copilot for Security Plugin for Splunk (Preview) ⓘ Cases	Set up
	CrowdSec Threat Intelligence (Preview) ⓘ IP addresses	Set up
	CyberArk (Preview) Plugin allows interaction with CyberArk SaaS services for managing privileged accounts.	Set up
	Cyware Respond (Preview) Automated Incident Response and threat analysis platform informed by extensive data visibility and advanced correlation to drive intelligent action from cybersecurity teams.	Set up
	Darktrace (Preview) Skills that interact with the Darktrace API.	Set up
	GreyNoise Community (Preview) ⓘ IP addresses	Set up
	GreyNoise Enterprise (Preview) ⓘ IP addresses, RIOT information, and GNQL queries	Set up

| Automation with Security Copilot

You can connect with Security Copilot using Logic Apps and Power Automate/Power Apps

Implement as part of your existing integrations – SC is 'just' an API that you access through a Connector.



| Cost of Security Copilot



Fixed cost per SCU is \$4/hour.

No per user licensing, or other cost associated.

# of SCUs	Per month	Per year	Notes
1	\$2,880	\$34,560	Minimum

| Cost of Security Copilot



Fixed cost per SCU is \$4/hour.

No per user licensing, or other cost associated.

# of SCUs	Per month	Per year	Notes
1	\$2,880	\$34,560	Minimum
3	\$8,640	\$103,680	Recommended for production

| Cost of Security Copilot



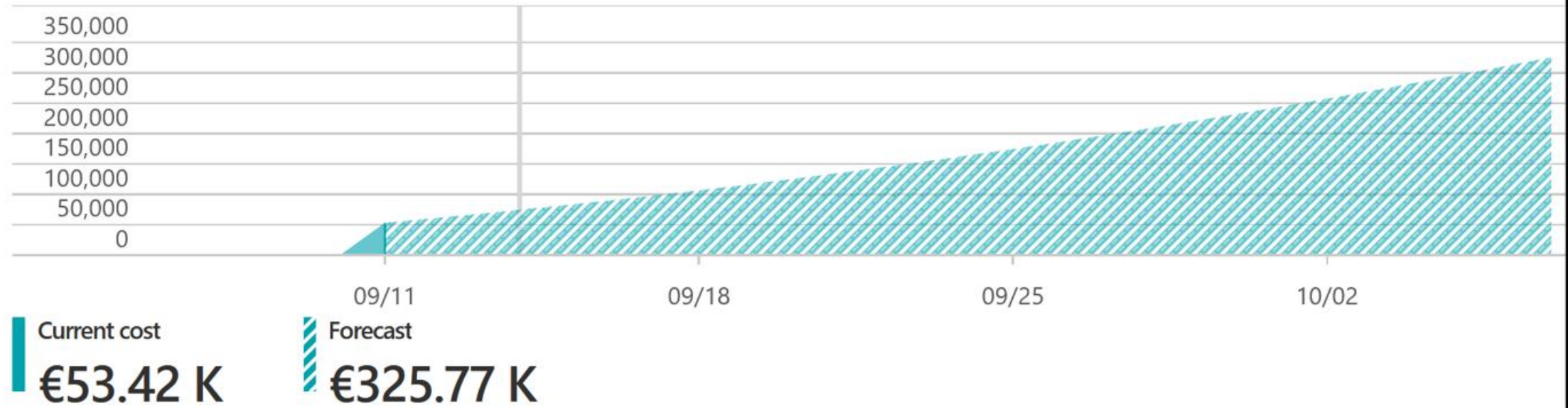
Fixed cost per SCU is \$4/hour.

No per user licensing, or other cost associated.

# of SCUs	Per month	Per year	Notes
1	\$2,880	\$34,560	Minimum
3	\$8,640	\$103,680	Recommended for production
10	\$28,800	\$345,600	Now you're serious

So, a quick story on cost management

Spending rate and forecast



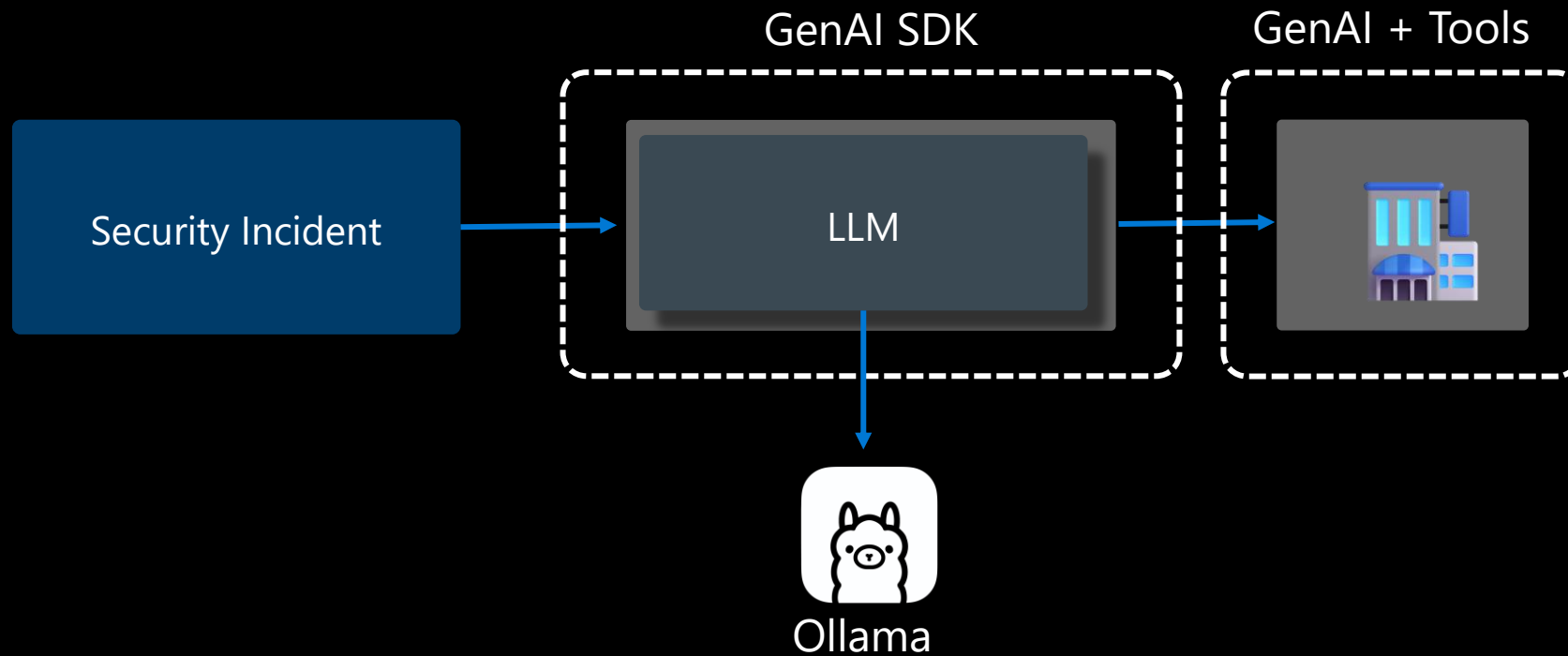
| What if you want to build your own?





DEMO: Agents in Copilot Studio

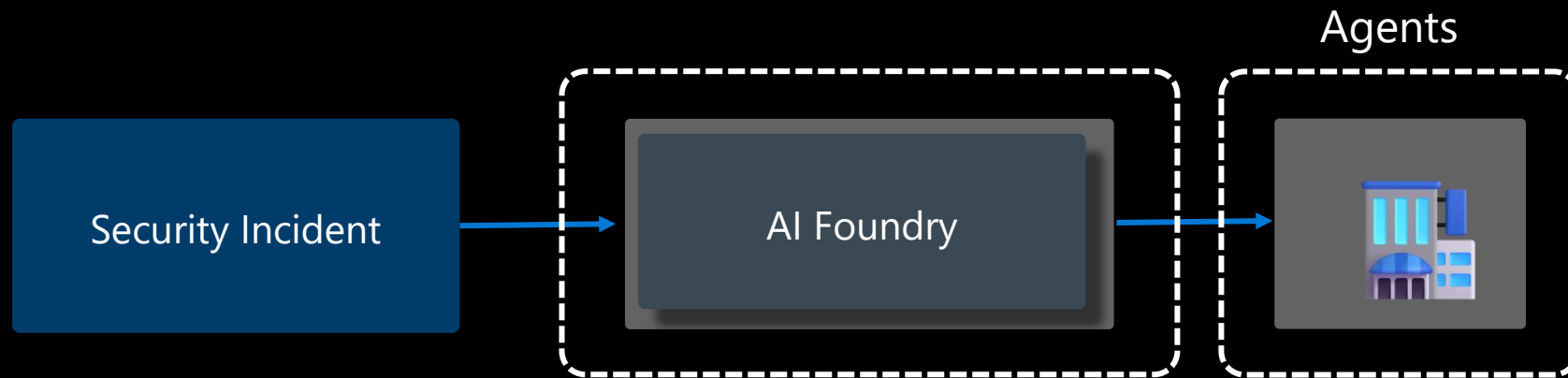
| What if you actively dislike the cloud?





DEMO: Run it locally

| And what if you love coding and troubleshooting?





DEMO: Azure AI Foundry + Agents

| End-to-end blueprint for Security + AI



Work on these during 2025



Strong foundation:
AD, Entra ID, identities,
authentication, authorization.



Understand
LLM capabilities, differences,
use and limitations.



Try to automate
everything: Logic Apps,
autonomous agents,
injecting GenAI
in between.

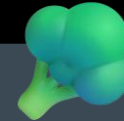


Follow up on
Security Copilot,
plugins and evolving
capabilities.

Use Ollama locally



Master at least one
SDK for GenAI:
LangChain, Semantic Kernel,
Microsoft.Extensions.AI



Kick back, relax,
eat a bit of broccoli
and find success.

| Resources

[Adoption Hub for Security Copilot](#)

[Complete Security Ninja for Security Copilot](#)

[Sample code from Microsoft](#)

[Custom plugins \(GitHub tutorial\)](#)

[How to build security plugins](#)

[Connect organizational knowledge base](#)

[Getting started with Microsoft.Extensions.AI](#)

[Ollama – essentials](#)

[Copilot Studio agents](#)

Thank you!



aka.ms/jussi

