

# Enhance your SOC team capabilities with Microsoft Copilot for Security

Mario Cuomo









## who am I



- **Mario Cuomo**
- **cloud solution architect**  
Security Tech Strategy team
- **based in Rome, 26 years old**
- **focusing on XDR + SIEM solutions**

## Agenda

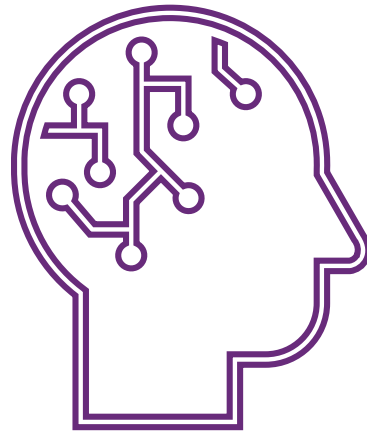
- 
- 
-  *Microsoft Copilot for Security* 🕶️
- 
- 

# Microsoft Copilot for Security

the first generative AI security product that empowers IT Operations and SOC analysts to defend their organizations at machine speed and scale

# artificial intelligence 101

the capability of a computer system to mimic *human-like cognitive functions* such as learning and problem-solving



## different types of AI techniques

- knowledge mining
- anomaly detection
- computer vision
- natural language processing
- machine learning
  - supervised learning
  - unsupervised learning
  - reinforcement learning
  - deep learning

## example – machine learning

*“a computer program is said to learn from experience **E** with respect to some class of tasks **T** and performance measure **P**, if its performance at tasks in **T**, as measured by **P**, improves with experience **E**.”*

Tom M. Mitchell



## example – machine learning types

### supervised learning

- *regression*
- *classification*

### unsupervised learning

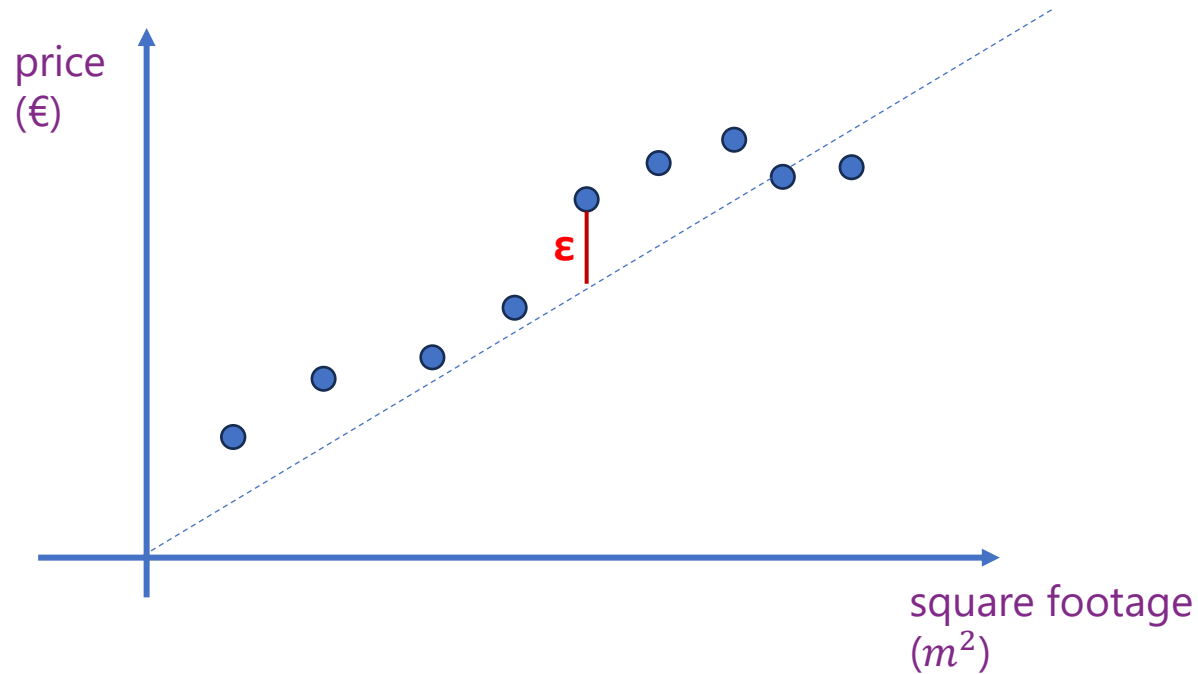
- *clustering*

### reinforcement learning

- *game theory*

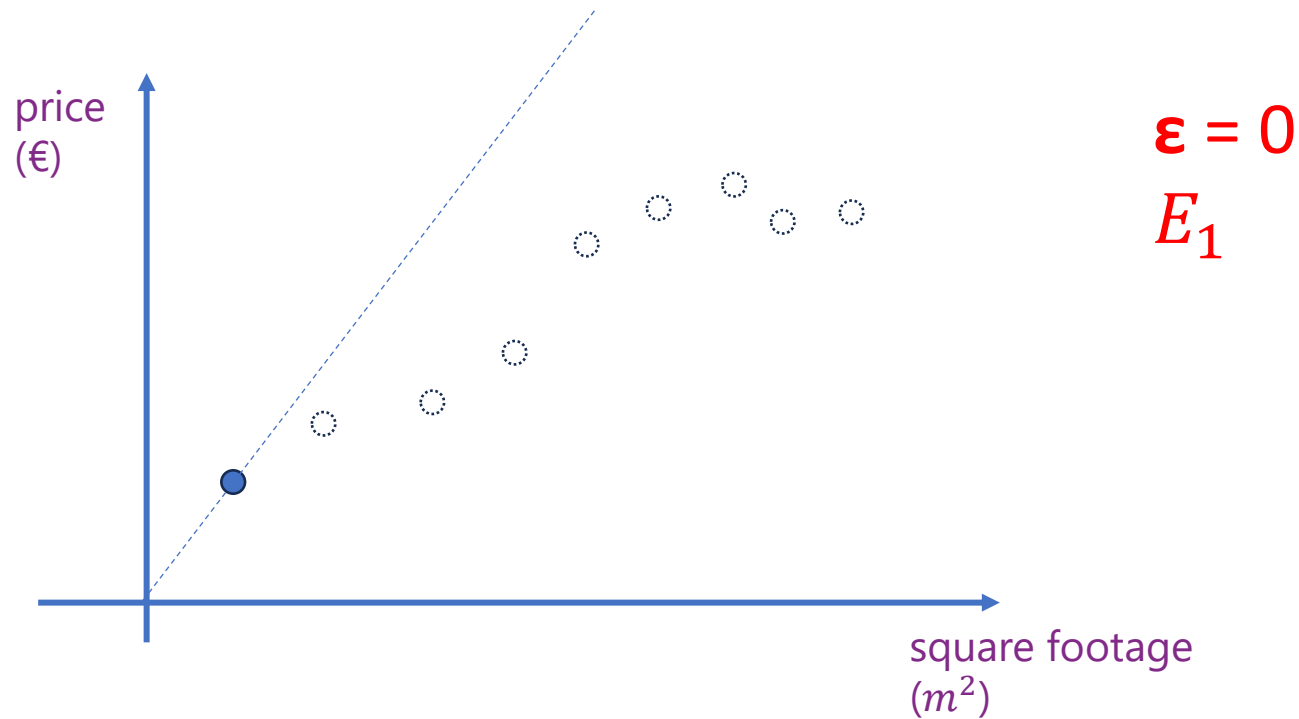
## example – machine learning regression

task **T**: estimate the cost of a house based on square footage



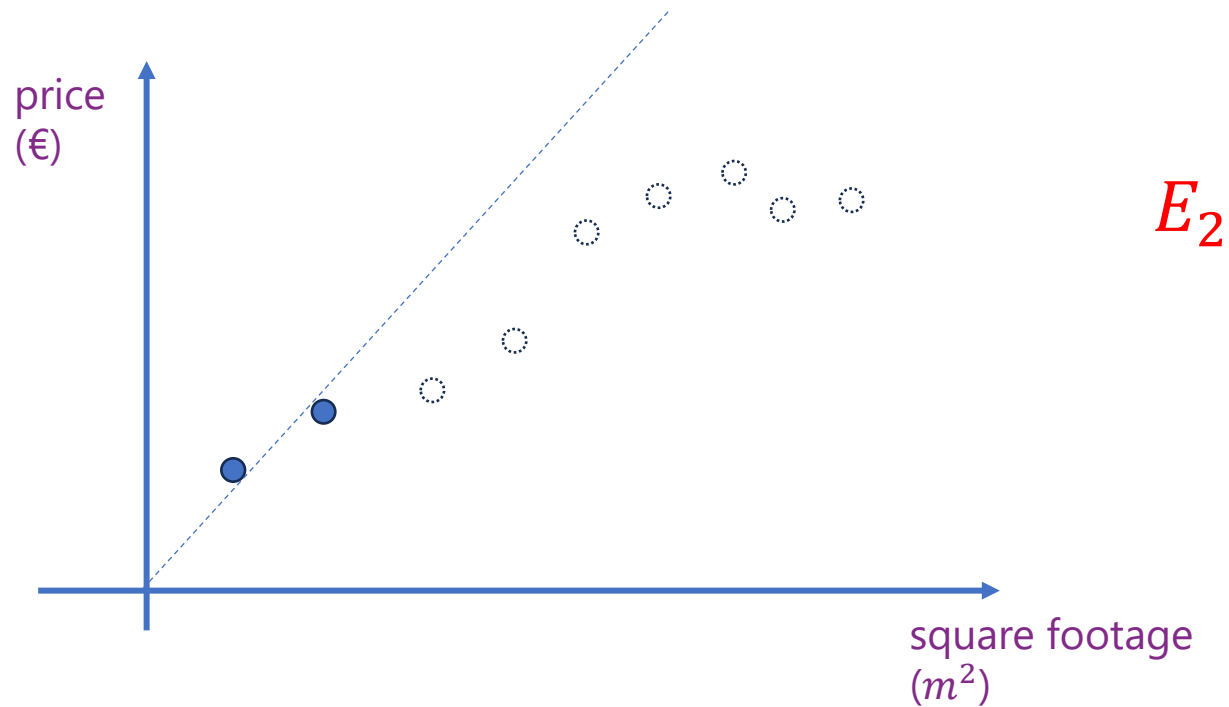
## example – machine learning regression

task **T**: estimate the cost of a house based on square footage



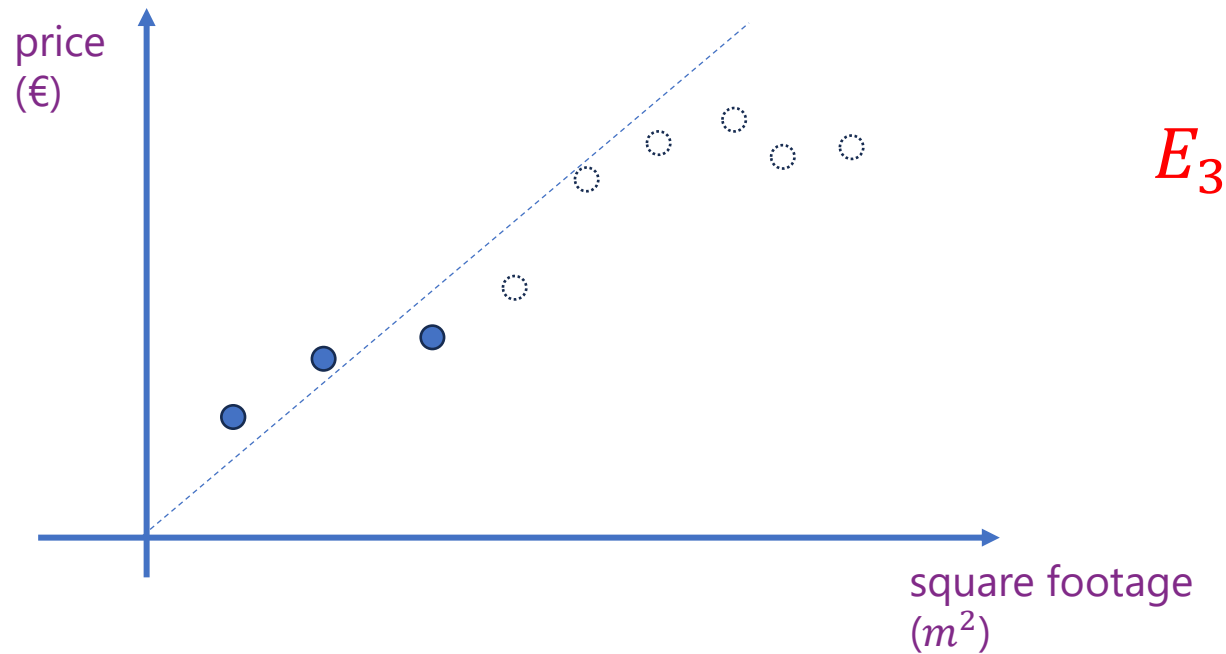
## example – machine learning regression

task **T**: estimate the cost of a house based on square footage







## example – machine learning regression

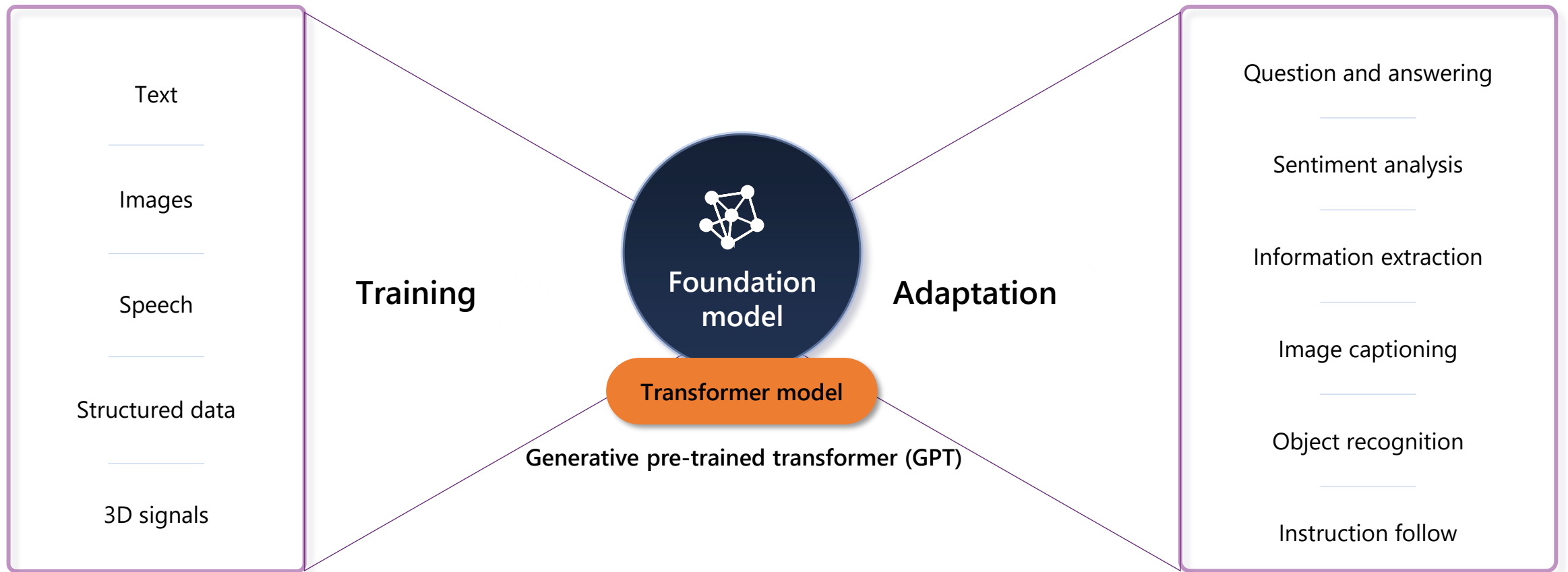
task **T**: estimate the cost of a house based on square footage



## A different AI model for each task!

- knowledge mining —————→ 
  - anomaly detection —————→ 
  - computer vision —————→ 
  - natural language processing
  - machine learning
    - supervised learning
    - unsupervised learning
    - reinforcement learning
    - deep learning —————→ 
- .....

## foundation model is the way



### Microsoft 365 Copilot

Works alongside you in the apps you use every day

### Dynamics 365 Copilot

Turbocharge your workforce with a copilot for every job role

### Copilot in Power Platform

Imagine it, describe it, and Power Platform builds it

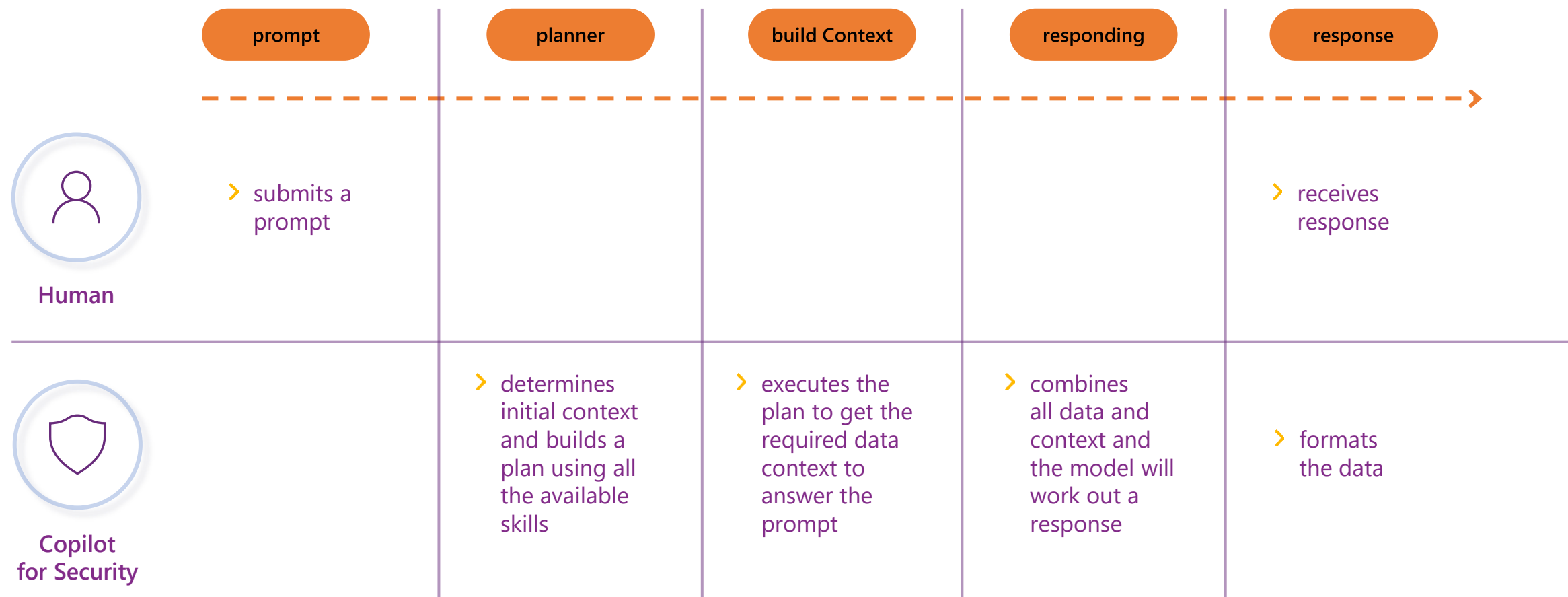
### Microsoft Copilot for Security

Defend at machine speed with Microsoft Copilot for Security

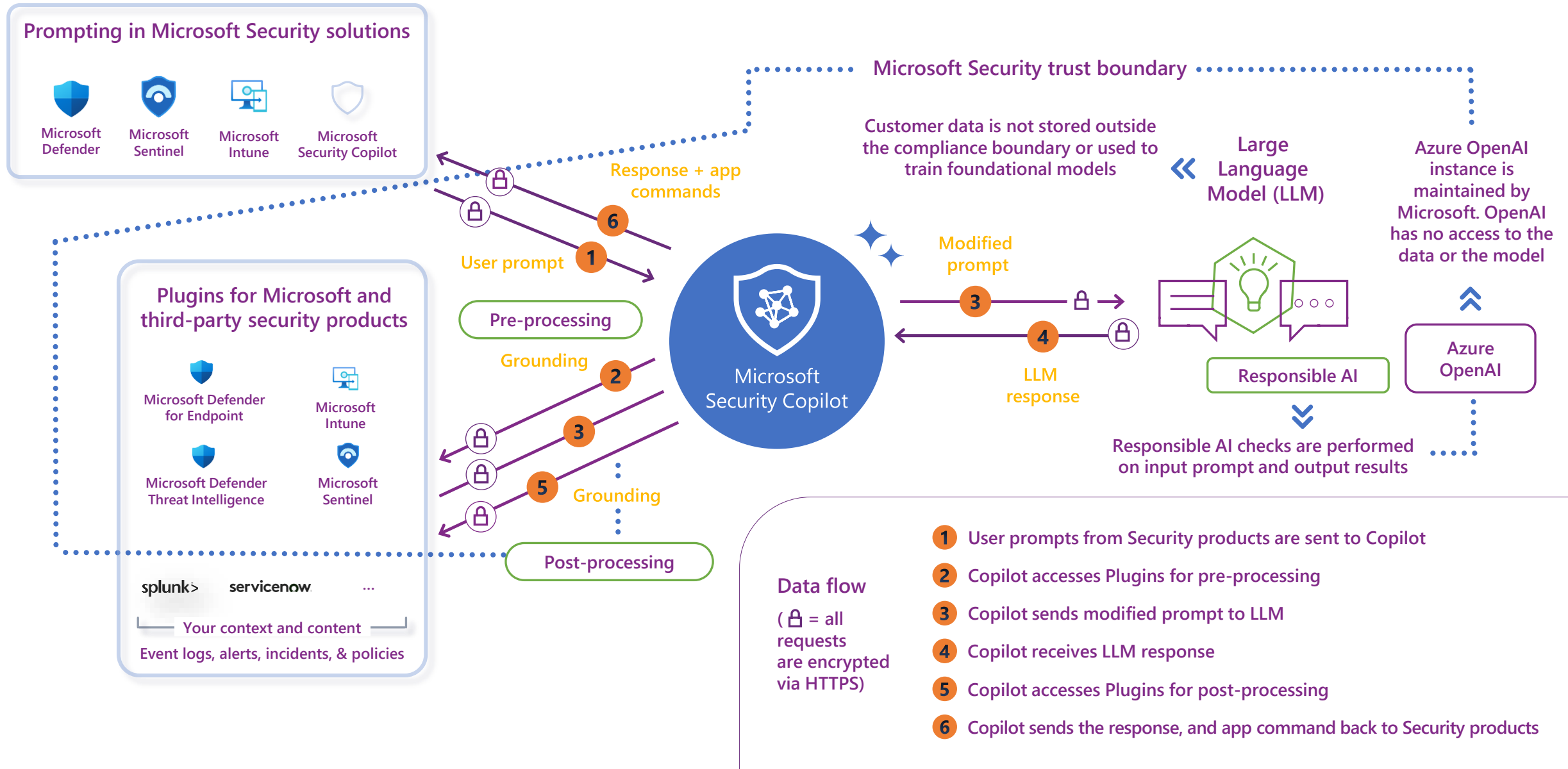
### GitHub Copilot

Increase developer productivity to accelerate innovation

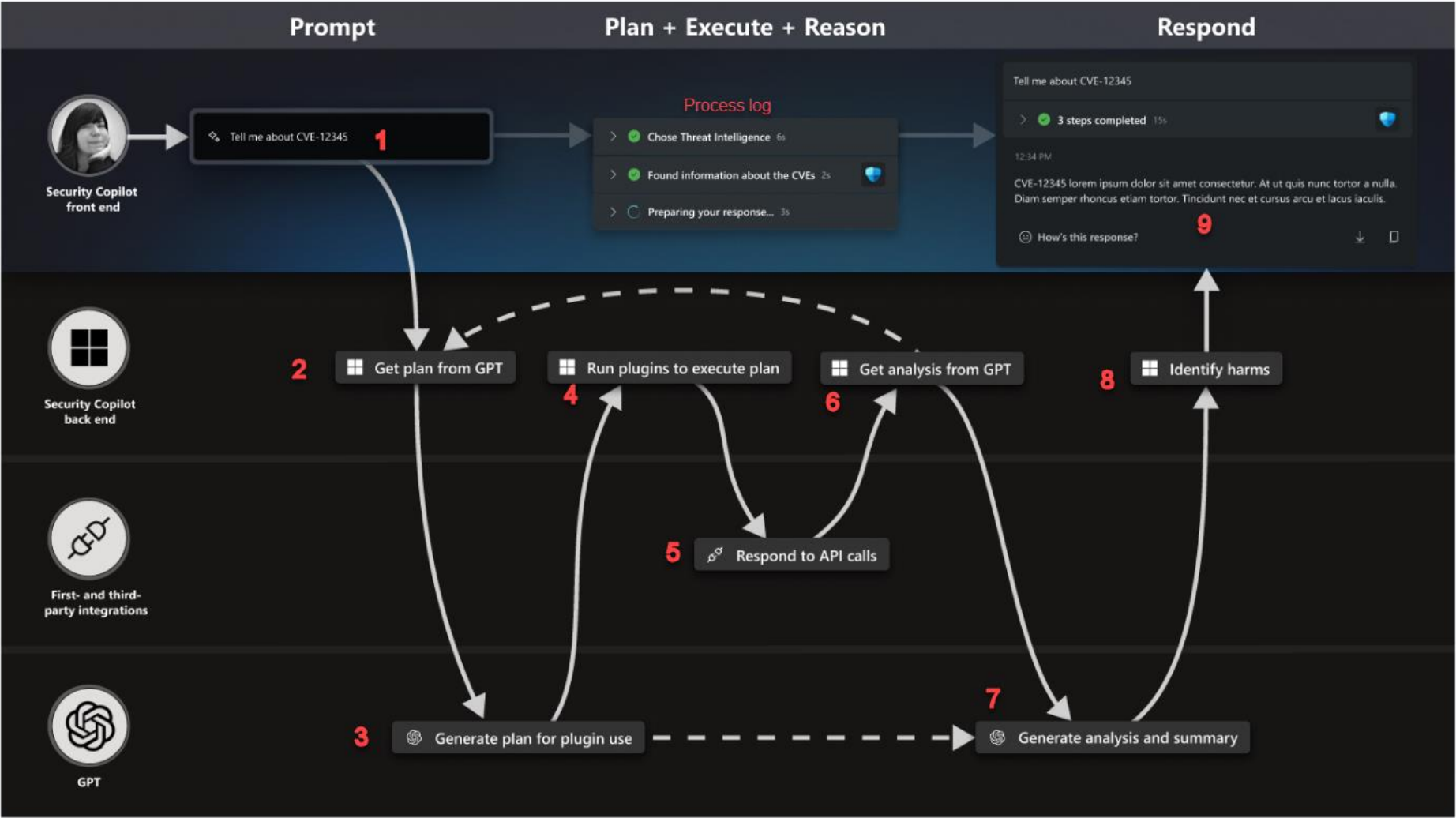




# enhance your soc team capabilities with Microsoft Copilot for Security



*enhance your soc team capabilities with Microsoft Copilot for Security*



# plugins

they represent a set of functionality that Copilot for Security can perform.

2 types

- preinstalled
  - Microsoft plugins
  - other plugins (ServiceNow)
  - websites
- custom

## Microsoft plugins

- Microsoft Entra
- Microsoft Defender External Attack Surface Management
- Microsoft Intune
- Microsoft Defender XDR
- Microsoft Sentinel
- Microsoft Defender Threat Intelligence
- Natural language to Microsoft Defender XDR KQL

## other plugins

- ServiceNow
- Splunk
- other plugins in the near future, working with *Microsoft Security Design Advisor Council Partners*

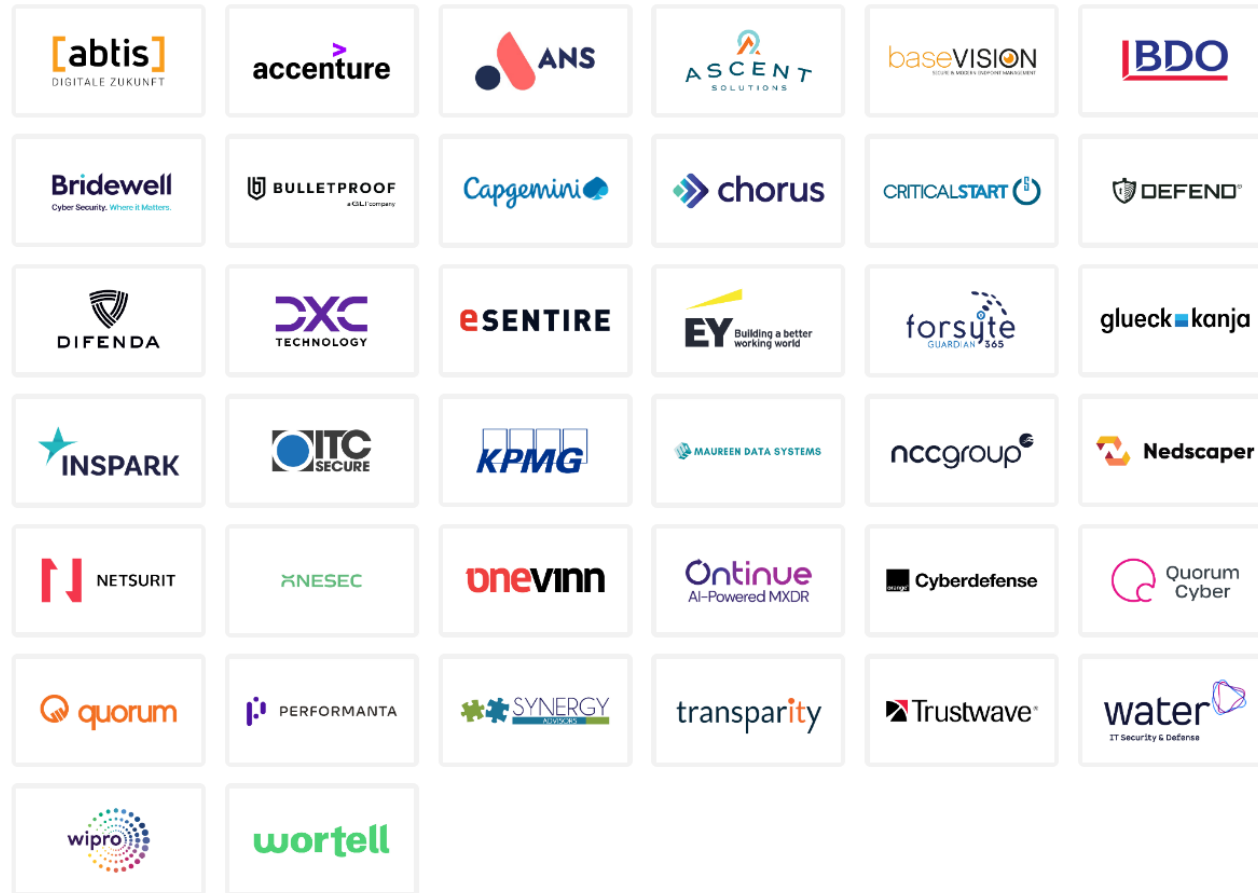
<https://securitypartners.transform.microsoft.com/copilot-private-preview-partners>

## Microsoft Security Design Advisor Council Partners



# Partner Private Preview

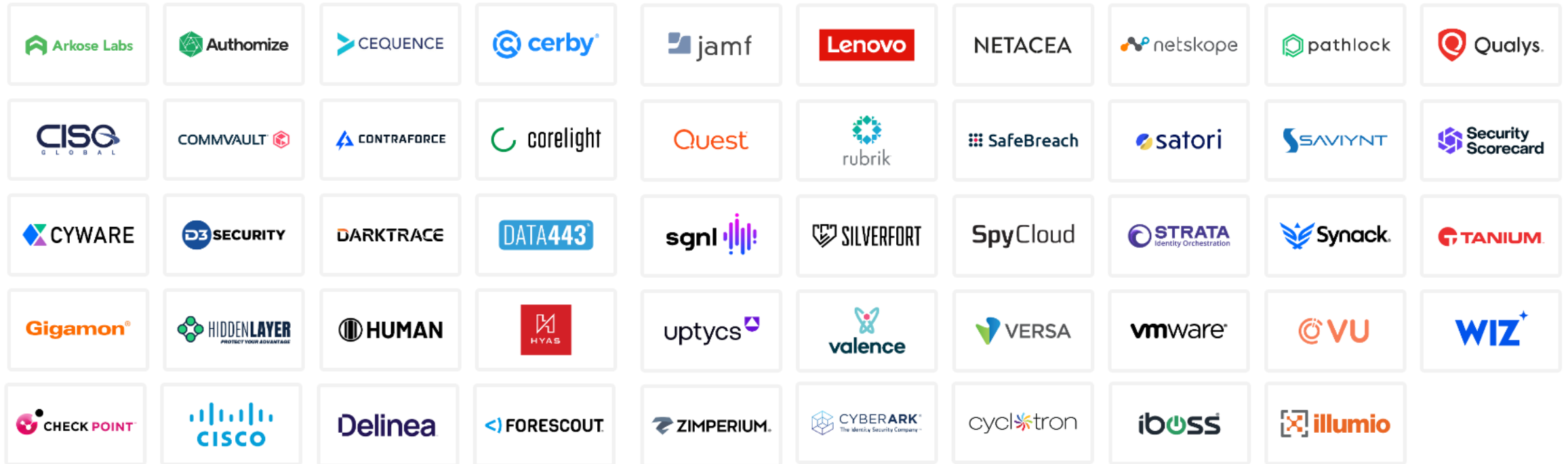
## Managed Security Service Providers





# Partner Private Preview

## Independent Software vendors



## websites

- authoritative sources like
  - Microsoft documentation
  - Mitre & Attack
  - CISA alerts & advisories
  - ...

## custom Plugins

defined using a YAML or JSON formatted manifest which describes metadata about the skill set and how to invoke the skills.

two required top level keys:

- Descriptor ---> metadata
- SkillGroups ---> what the plugin is able to perform

# how to interact with Copilot for Security

you can interact with Copilot for Security using

- standalone portal  
single portal [www.securitycopilot.microsoft.com](https://www.securitycopilot.microsoft.com) to interact with all the connected datasources
- embedded experiences  
Copilot for Security integrated in different security product portals to have ad hoc capabilities ready to be used

# DEMO TIME

## demo

- standalone portal
- interactive tour
- manage plugins

## embedded Experience – Defender 365

- summarize an incident
- guided incident response
- analyze a script
- generate KQL from natural language
- create incident reports

# embedded experience – Defender 365

## summarize an incident

Incidents > Multi-stage incident involving Execution & Lateral movement including Ransomware on multiple endpoints reported by multiple sources



### Multi-stage incident involving Execution & Lateral...

Security Copilot

Ask Defender Experts

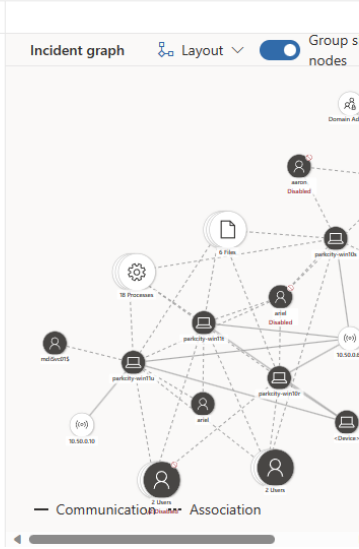
Comments and history

Important! Attack disruption has automatically taken multiple response actions. For more details, go to the [Action center](#).

This information is limited because of your current permission. Contact a global administrator to change your permissions.

Attack story Alerts (65) Assets (16) Investigations (15) Evidence and Response (64) Summary

- #### Alerts
- 41/65 Active alerts Unpin all Show all
- Oct 24, 2023 6:58 PM • New  
**User created or modified an account that later performed malicious activity**  
3 Users
  - Oct 24, 2023 6:58 PM • New  
**User was created or modified by a compromised account**  
2 Users
  - Oct 24, 2023 7:02 PM • New  
**User was created or modified by a compromised account**  
2 Users
  - Oct 24, 2023 7:03 PM • New  
**Suspicious additions to sensitive groups**  
4 Devices 3 Users
  - Oct 25, 2023 12:23 AM • New  
**Potential human-operated malicious activity**



### Multi-stage incident involving Execution & Lateral movement including Ransomware on multiple endpoints reported by multiple sources

High Active

Ransomware Attack Disruption AlpineSkiHouse

Manage incident

#### RECOMMENDATIONS

##### Ransomware Incident response playbook

View ransomware investigation and response recommended steps for this incident

Open ransomware playbook

#### Security Copilot

##### Incident summary

Oct 25, 2023 3:44 PM

The security incident occurred between 2023-10-24 07:58:00 UTC and 2023-10-24 20:01:13 UTC, involving high-severity alerts and multiple devices. The incident began with group membership changes for users Aaron Voski and Ariel Kai, impacting users 'steve', 'aaron', and 'ariel'. These changes were made by a compromised account, leading to malicious activity.

Steve Lewis, the IT director, added two accounts to the sensitive Domain Admins group, raising suspicion. Potential human-operated malicious activities were detected on several Windows 10 and Windows 11 devices, involving processes such as cmd.exe and PSEXESVC.exe. These activities impacted users 'ariel', 'steve', and 'aaron', and were associated with lateral movement, ransomware, and suspicious activity kill chain stages.



# embedded experience – Defender 365


## guided incident response




The screenshot displays the Microsoft Defender 365 Security Center interface, specifically the 'Incidents' section. The main title is 'Multi-stage incident involving Initial access & Collection involving multiple users r...'. The interface is divided into several panels:

- Alerts:** A list of alerts on the left, including 'User accessed link in ZAP-quarantined email', 'A potentially malicious URL click was detected', 'Email messages containing malicious URL removed after delivery', 'Suspicious inbox forwarding rule', 'Activity from a Tor IP address', 'Creation of forwarding/redirect rule', 'Suspicious email forwarding rule', and 'Activity from a Tor IP address'.
- Incident graph:** A central graph showing the relationships between various entities. It includes nodes for 'Microsoft Exchange Online', '2 Cloud Applications', '2 IPs', and 'EXTERNAL Full mailbox notice'. The graph is labeled 'Communication' and 'Association'.
- Incident details:** A panel on the right showing the incident's details, including 'Assigned to', 'Incident ID', and '18823'.
- Security Copilot:** A panel on the right providing AI-generated insights and recommendations. It includes sections for 'Guided response', 'Triage', and 'Remediation'. The 'Guided response' section is highlighted with a red box and contains the following steps:
  - Triage:** Confirm this is a 'true positive'. Other organizations tend to classify similar incidents as a 'true positive'. (Buttons: Classify, View similar incidents)
  - Remediation:** Delete similar emails. We found emails that are very similar to emails involved in this incident. Delete these emails to contain the attack. (Buttons: Soft delete emails, View similar emails)
  - Reset password for:** The user clicked a known phishing link. Require them to change their password to address possible compromise. (Buttons: Reset user password)

# embedded experience – Defender 365

## analyze a script

 **Multi-stage incident involving Privilege escalation...**

 Security Copilot  Ask Defender Experts  Comments and history

This information is limited because of your current permission. Contact a global administrator to change your permissions.

**Attack story** Alerts (74) Assets (17) Investigations (1) Evidence and Response (46) Summary

**Alerts**  
0/74 Active alerts  
Unpin all Show all

Oct 25, 2023 11:56 AM Resolved  
**Activity from a Tor IP address**  
Backup Admin (Parkcity)

Oct 25, 2023 11:56 AM Resolved  
**Logon from a risky IP address**  
Backup Admin (Parkcity)

Oct 25, 2023 11:56 AM Resolved  
**System recovery setting tampering**  
ec2amaz-9mdsbs4

Oct 25, 2023 11:58 AM Resolved  
**Logon from a risky IP address**  
Backup Admin (Parkcity)

Oct 25, 2023 11:59 AM Resolved  
**Possible ransomware activity based on a known malicious extension**  
ec2amaz-9mdsbs4 SYSTEM

Oct 25, 2023 12:03 PM Resolved  
**Ransomware behavior detected in the file system**  
ec2amaz-9mdsbs4 SYSTEM

**Ransomware behavior detected in the file system**  
Clear selection

**Incident graph** Layout Group similar nodes

Communication Association

11:56:12 AM [9196] CustomScriptHandler.exe "enable"

11:56:16 AM [4268] cmd.exe "cmd" /C powershell -ExecutionPolicy Unrestricted -EncodedCommand DQAKACMAIABTAGEAdgBIACAAAdBoAGUAIABSAGEAbgBzAG8AbQAgAEQAZQBzAGsAdABvAHAIAIABCAGEAYwBrAGcAcgBvAHUAbgBkAA0ACnAkAFQAZQZRTAHAALIArBhAHQAAaAAAD0AIAAIAFMACOnRrAHcAaOR

11:56:17 AM [752] powershell.exe powershell -ExecutionPolicy Unrestricted -EncodedCommand DQAKACMAIABTAGEAdgBIACAAAdBoAGUAIABSAGEAbgBzAG8AbQAgAEQAZQBzAGsAdABvAHAIAIABCAGEAYwBrAGcAcgBvAHUAbgBkAA0ACnAkAFQAZQZRTAHAALIArBhAHQAAaAAAD0AIAAIAFMACOnRrAHcAaOR



**Analyze**


powershell -ExecutionPolicy Unrestricted -EncodedCommand DQAKACMAIABTAGEAdgBIACAAAdBoAGUAIABSAGEAbgBzAG8AbQAgAEQAZQBzAGsAdABvAHAIAIABCAGEAYwBrAGcAcgBvAHUAbgBkAA0ACnAkAFQAZQZRTAHAALIArBhAHQAAaAAAD0AIAAIAFMACOnRrAHcAaOR

**Analyze**

Start-Process bcdedit -ArgumentList "/set recoveryenabled no"  
Start-Process bcdedit -ArgumentList "/set bootstatuspolicy ignoreallfailures"

Process id 752

 **Script analysis**

3. Disable recovery options and delete shadow copies.

[Hide code](#)

```
Start-Process bcdedit -ArgumentList "/set recoveryenabled no"  
Start-Process bcdedit -ArgumentList "/set
```

4. Iterate through the folders and encrypt the files by renaming them with a ".quantum" extension and adding a string "Are you kidding?!" to the content.

[Hide code](#)

```
ForEach ($i in $Folders) { ... }
```

5. Create "SAVE\_YOUR\_FILES.txt" files on the user's desktop with a ransom message.

[Hide code](#)

```
"Your files in this Folder are encrypted with a key you will never find`n Email us at LulzCrypt@signalme.net" | Out-File
```

6. Set the ransom desktop background and restart the explorer process

# embedded experience – Defender 365

generate KQL from natural language

The screenshot displays the Microsoft Defender 365 Advanced Hunting interface. On the left, a sidebar lists various data sources under categories like 'Alerts & behaviors', 'Apps & identities', and 'Email & collaboration'. The main area shows a KQL query for finding device logon events for a user named 'steve'. The query is: `DeviceLogonEvents | where AccountName == "steve" | summarize arg_max(Timestamp, *) by DeviceName`. Below the query, the 'Results' tab shows a table with 6 items, including columns for DeviceName, Timestamp, DeviceId, ActionType, and LogonType. A 'Security Copilot' overlay is visible on the right, showing a chat interface where a user's natural language request is converted into the KQL query shown in the main interface.

**Advanced hunting**

New query + Create new X Clear all queries

Schema Functions Queries ...

Search

**Alerts & behaviors**

- AlertInfo
- AlertEvidence
- BehaviorInfo
- BehaviorEntities

**Apps & identities**

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta

**Email & collaboration**

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents
- UrlClickEvents

**Query**

Run query Save Share link Security Copilot

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
1 DeviceLogonEvents
2 | where AccountName == "steve"
3 | summarize arg_max(Timestamp, *) by DeviceName
4
```

**Results**

Export 6 items Search 0:0.159 Low

DeviceName	Timestamp	DeviceId	ActionType	LogonType
parkcity-dc.parkcity.alpir	Oct 26, 2023 2:44:45 PM	d479754249844c030cd1	LogonSuccess	Network
parkcity-win10b.parkcity	Sep 28, 2023 5:26:36 PM	172c9a92ee50cb7943e0	LogonSuccess	Remote
parkcity-win10s.parkcity	Oct 25, 2023 8:56:23 PM	adfd6fe3140a9be15052	LogonSuccess	Remote
parkcity-win10r.parkcity	Oct 25, 2023 6:48:27 AM	a05ae3475cf1cffe01e4c	LogonSuccess	Network

**Security Copilot**

Oct 26, 2023 2:55 PM

show device logon events for account name steve and the most recent logon event for each device

Oct 26, 2023 2:56 PM

Here's a query you can use to find what you need:

```
DeviceLogonEvents
| where AccountName == "steve"
| summarize arg_max(Timestamp, *)
by DeviceName
```

Add and run


AI generated. Verify for accuracy.

Ask a question to generate a query


# embedded experience – Defender 365


## incident report

Incidents > Multi-stage incident involving Execution & Lateral movement including Ransomware on multiple endpoints reported by multiple sources

 **Multi-stage incident involving Execution & Latera...**

Security Copilot ? Ask Defender Experts Comments and history ...

 Important! Attack disruption has automatically taken multiple response actions. For more details, go to the [Action center](#).

 This information is limited because of your current permission. Contact a global administrator to change your permissions.

Attack story Alerts (65) Assets (16) Investigations (15) Evidence and Response (64) Summary

**Alerts**

41/65 Active alerts Unpin all Show all

Oct 24, 2023 6:58 PM • New

User created or modified an account that later performed malicious activity

3 Users

Oct 24, 2023 6:58 PM • New

User was created or modified by a compromised account

2 Users

Oct 24, 2023 7:02 PM • New

User was created or modified by a compromised account

2 Users

Oct 24, 2023 7:03 PM • New

Suspicious additions to sensitive groups

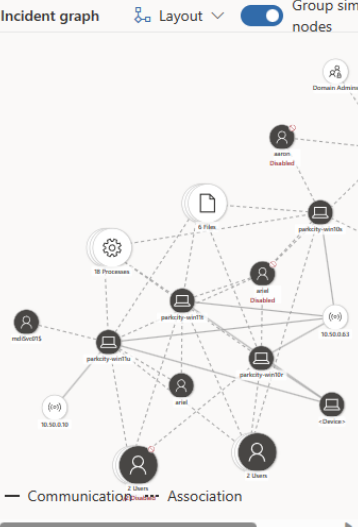
4 Devices 3 Users

Oct 25, 2023 12:23 AM • New


Potential human-operated malicious activity

Incident graph

Layout Group sim nodes



Communication Association

 **Multi-stage incident involving Execution & Lateral movement including Ransomware on multiple endpoints reported by multiple sources**

High Active

Ransomware Attack Disruption AlpineSkiHouse

Manage incident

**RECOMMENDATIONS**

Ransomware Incident response playbook

View ransomware investigation and response recommended steps for this incident

Open ransomware playbook

**Incident report**

Incident report Oct 25, 2023 3:49 PM

Incident title

Multi-stage incident involving Execution & Lateral movement including Ransomware on multiple endpoints reported by multiple sources

Incident details

Analysts

Time created 10/24/2023 07:58:00

First log

Last log

Time closed

Incident summary

The security incident occurred between 2023-10-24 07:58:00 UTC and 2023-10-24 20:01:13 UTC, involving high-severity alerts and multiple devices. The incident began with group membership changes for users Aaron Voski and Ariel Kai, which led to the creation of accounts that performed malicious activities. The

# DEMO TIME

## demo

- summarize an incident
- guided incident response
- analyze a script
- generate KQL from natural language
- create incident reports

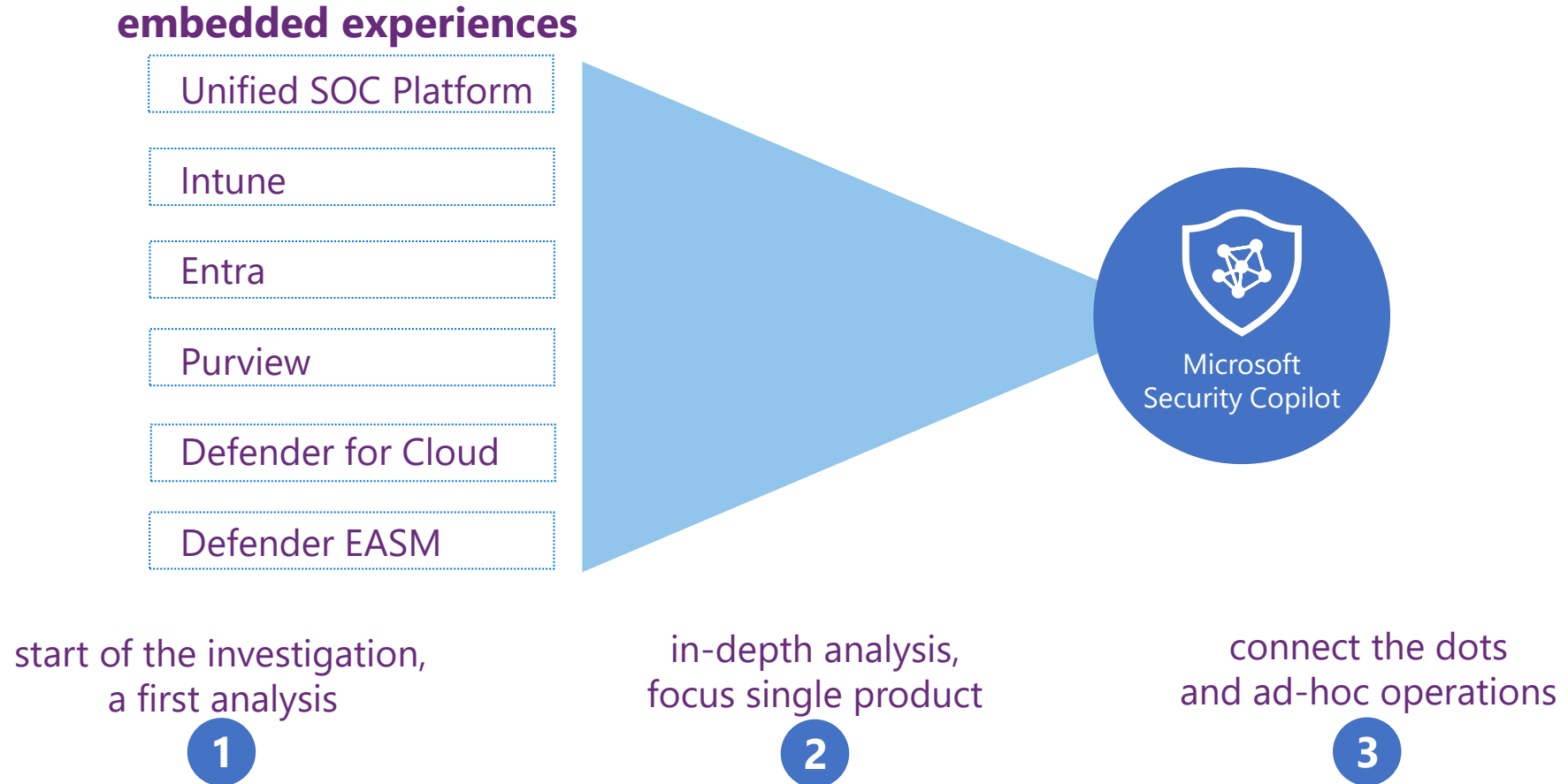
## standalone vs embedded experience

standalone vs embedded experience

# **COPILOT FOR SECURITY IS NOT A TOOL THAT EXTENDS YOUR SECURITY LAYERS**



# standalone vs embedded experience



## sessions

each interaction with Copilot for Security can be performed in the context of an existing or new session.

### My sessions

AllRecent

Delete

<input type="checkbox"/> Name	Updated	Created
<input type="checkbox"/> Vulnerability impact assessment - CVE-2023-24329	4 days	6 days
<input type="checkbox"/> GetEntraRiskyUsers	4 days	4 days
<input type="checkbox"/> ScriptAnalyzer	4 days	4 days
<input type="checkbox"/> Incident summary for incident 19188	6 days	6 days
<input type="checkbox"/> Threat actor profile	11 days	11 days

...

Duplicate

Delete

Edit name

+ New session

## sessions

sessions are used to organize prompts & responses related to a specific investigation

- return to an existing session
- edit & re-run queries
- give meaningful names
- delete when no longer required
- exported
- shared

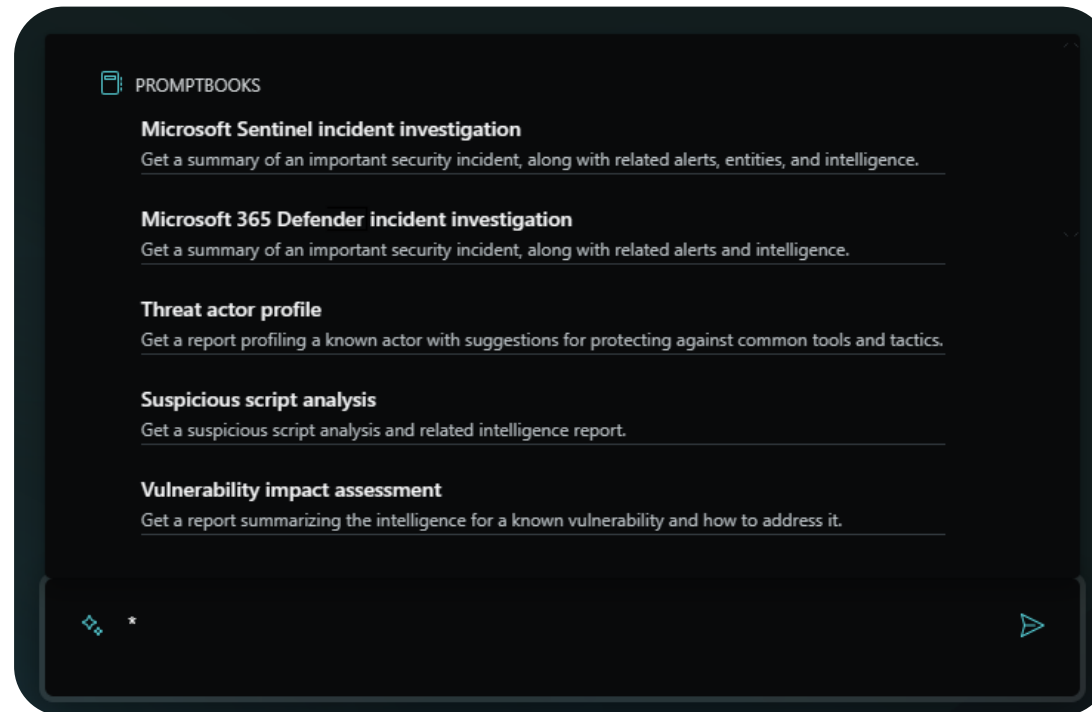
## sessions

Copilot for Security uses OAuth 2.0 On-Behalf-Of flow  
users can only query against data they have access to!

Role	Run prompts	Run promptbooks	Manage plugins	Configure settings	Opt-in or opt-out on product and model improvements and model improvements
Global admin	✓*	✓*	✓	✓	✓
Global reader	✓*	✓*	--	--	--
Security admin	✓*	✓*	✓	✓	✓
Security operator/reader	✓*	✓*	--	--	--

# promptbooks

promptbooks are templates of bundled prompts put together to accomplish specific security-related tasks



# DEMO TIME





# *Questions & Answers*