Describe Microsoft Copilot for Security

Introduction

Completed100 XP

- 1 minute

Organizations face unprecedented challenges, in the rapidly evolving digital landscape, such as increasingly sophisticated cyber threats and a significant talent shortage in cybersecurity. Microsoft Copilot for Security is a cloud-based, AI-powered security analysis tool that is designed to address these challenges. It enables analysts to process security signals and respond to threats at a machine speed that far surpasses human capabilities, thus revolutionizing the way organizations approach cybersecurity.

After completing this module, you'll be able to:

- Describe what Microsoft Copilot for Security is.
- Describe the terminology of Microsoft Copilot for Security.
- Describe how Microsoft Copilot for Security processes prompt requests.
- Describe the elements of an effective prompt.
- Describe how to enable Microsoft Copilot for Security.

Get acquainted with Microsoft Copilot for Security

Completed100 XP

- 4 minutes

The top security challenges organizations face include:

- An increase in the number and sophistication of attacks.
- A talent shortage that is driving the need for automation, integration, and consolidation of security tools.

- Visibility into security, privacy, compliance, and governance.

Organizations need to act quickly to address all the security challenges they face, but working at human speed, even if there weren't a talent shortage, isn't enough. Organizations need to work at machine speed.

Microsoft Copilot for Security is an AI-powered, cloud-based security analysis tool that enables analysts to respond to threats quickly, process signals at machine speed, and assess risk exposure more quickly than may otherwise be possible.

Use cases

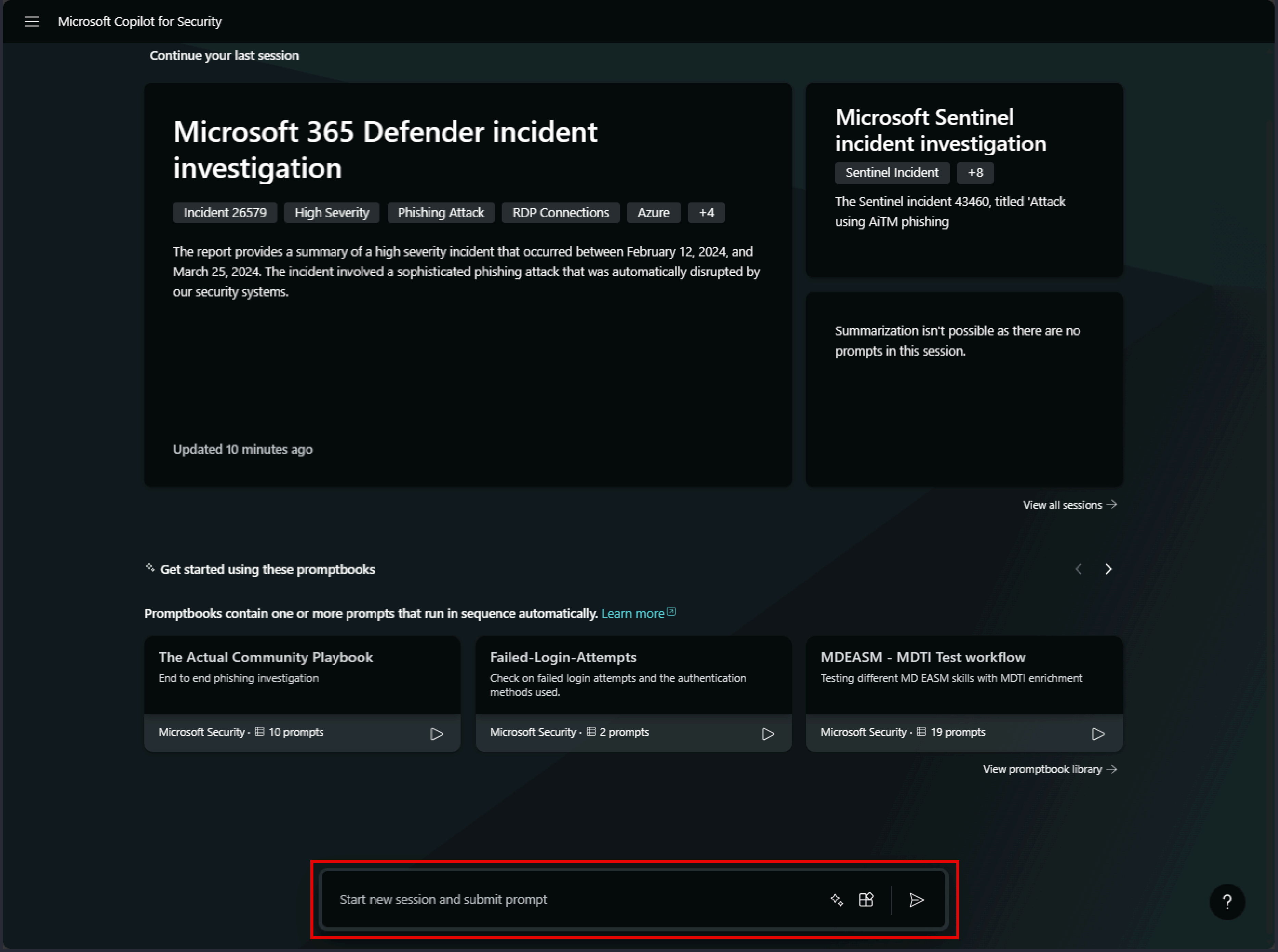
Microsoft Copilot for Security focuses on making the following highlighted use cases easy to use.

- 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.

These use cases represent just a few of the capabilities that Copilot delivers and that helps make analysts more productive and also helps up-level them.

Standalone and embedded experience

You can experience Copilot through the dedicated site, also referred to as the standalone experience. Users interact with Copilot through the prompt bar. In the prompt bar, users make requests in natural language and receive response outputs as text, images, or documents.



Continue your last session

Microsoft 365 Defender incident investigation

Incident 26579 | High Severity | Phishing Attack | RDP Connections | Azure | +4

The report provides a summary of a high severity incident that occurred between February 12, 2024, and March 25, 2024. The incident involved a sophisticated phishing attack that was automatically disrupted by our security systems.

Updated 10 minutes ago

Microsoft Sentinel incident investigation

Sentinel Incident | +8

The Sentinel incident 43460, titled 'Attack using AiTM phishing

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

View all sessions →

Get started using these promptbooks

Promptbooks contain one or more prompts that run in sequence automatically. Learn more

The Actual Community Playbook
End to end phishing investigation
Microsoft Security · 10 prompts

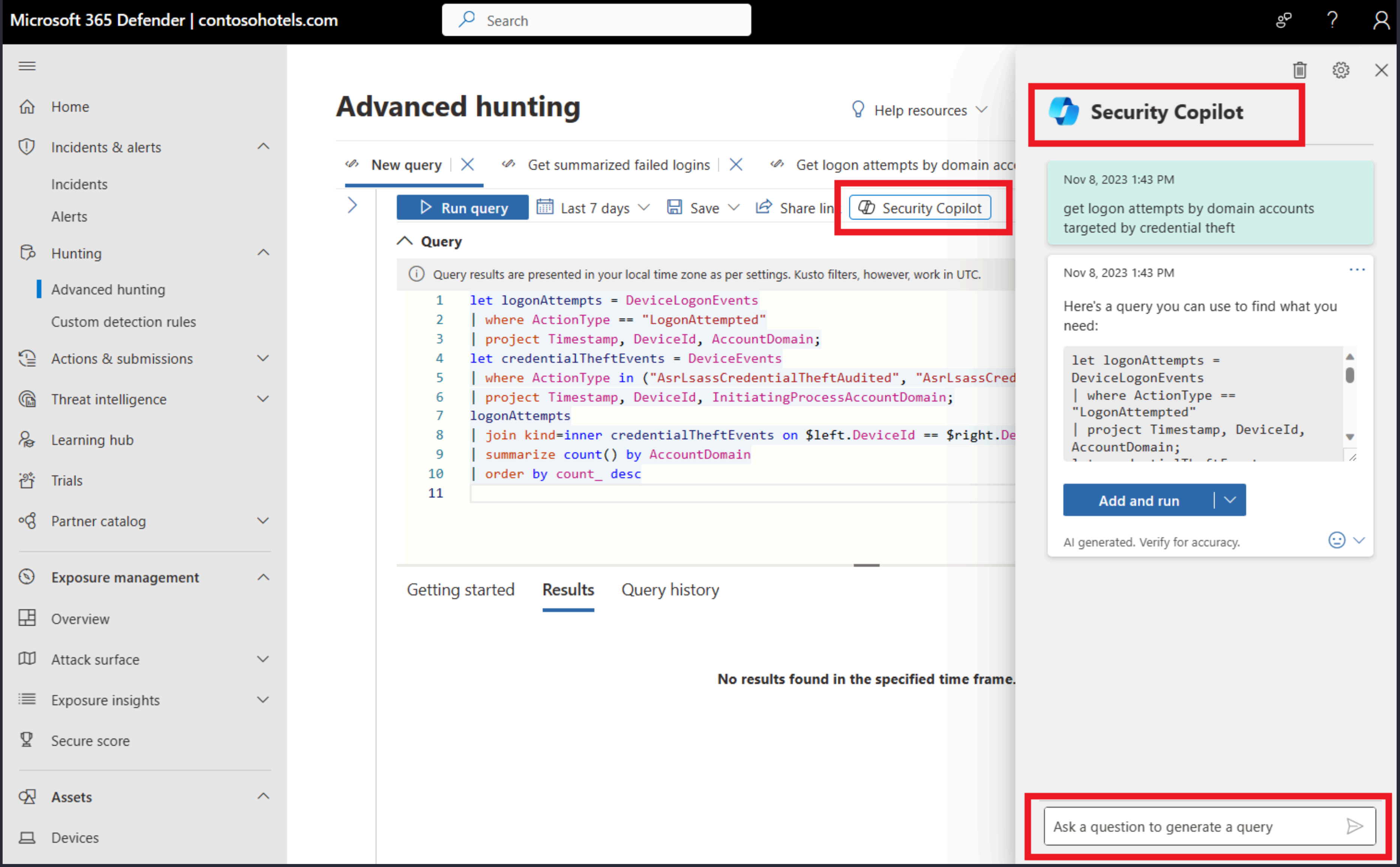
Failed-Login-Attempts
Check on failed login attempts and the authentication methods used.
Microsoft Security · 2 prompts

MDEASM - MDTI Test workflow
Testing different MD EASM skills with MDTI enrichment
Microsoft Security · 19 prompts

View promptbook library →

Start new session and submit prompt

Additionally, some Microsoft security products embed Copilot capabilities directly within the products' user interface. This experience is referred to as the embedded experience. Microsoft Defender XDR, for example, enables Copilot capabilities including summarizing incidents, analyzing scripts, generating KQL queries, and more.



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

```
let logonAttempts = DeviceLogonEvents
| where ActionType == "LogonAttempted"
| project Timestamp, DeviceId, AccountDomain;
let credentialTheftEvents = DeviceEvents
| where ActionType in ("AsrLsassCredentialTheftAudited", "AsrLsassCred
| project Timestamp, DeviceId, InitiatingProcessAccountDomain;
logonAttempts
| join kind=inner credentialTheftEvents on $left.DeviceId == $right.De
| summarize count() by AccountDomain
| order by count_ desc
```

No results found in the specified time frame.

Nov 8, 2023 1:43 PM

get logon attempts by domain accounts targeted by credential theft

Nov 8, 2023 1:43 PM

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

```
let logonAttempts =
DeviceLogonEvents
| where ActionType ==
"LogonAttempted"
| project Timestamp, DeviceId,
AccountDomain;
```

AI generated. Verify for accuracy.

Ask a question to generate a query

More information on both the standalone and embedded experience are covered in subsequent modules. Images shown throughout the rest of this module are based on the standalone experience.

Watch this short video for a summary of the users experiences that Microsoft Copilot for Security offers.

Natural language processing (NLP)

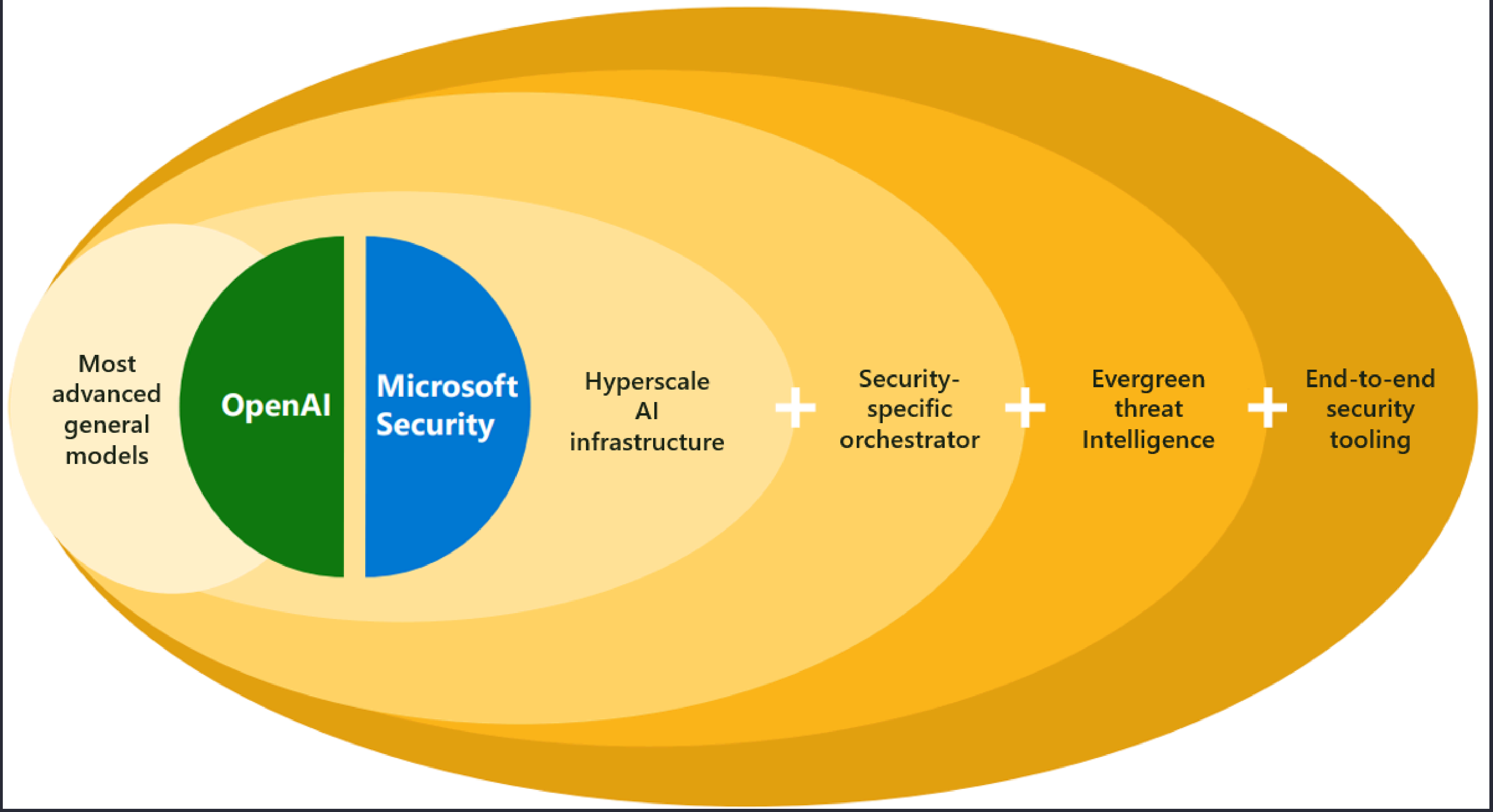
Copilot is built using Azure OpenAI Services and is designed to integrate with existing security tools and processes, making it easier for organizations to improve their overall security posture. Azure OpenAI Services provides REST API access to OpenAI's powerful large language models (LLMs) for natural language processing (NLP), while providing security capabilities of Microsoft Azure.

With access to the powerful LLMs for NLP, Copilot is able to read, decipher, and make sense of human languages, enabling users to securely interact with it using natural language. Although the LLMs are trained on a vast amount of information that endows Copilot with broad general knowledge and problem solving abilities, it’s not enough. Security analysts expect their copilot to be trained on security and that is where the integration with existing security tools and processes comes into play.

Integration with Security-specific sources

Copilot combines powerful LLMs with security-specific sources from Microsoft. These security-specific sources are informed by Microsoft’s unique global threat intelligence, more than 65 trillion daily signals, and incorporates information from a growing set of security solutions using plug-ins and connections to knowledge bases. Through plug-ins, Copilot integrates with Microsoft's own security products, non-Microsoft products, and open-source intelligence feeds. Connections to an organization's knowledge bases gives Copilot more context, resulting in responses that are more relevant, specific, and customized to the user. Through the powerful combination of advanced general models and security specific sources, Copilot is able to learn at machine speed to help analysts identify and respond to emerging threats.

The information you give Copilot will only be accessible to your organization. Your data is your data, and it's protected by comprehensive enterprise compliance and security controls. Your data isn't used to train the foundation AI models.


Most advanced general models
OpenAI
Microsoft Security
Hyperscale AI infrastructure
+
Security-specific orchestrator
+
Evergreen threat Intelligence
+
End-to-end security tooling

Microsoft Copilot for Security is the first security product to enable defenders to move at the speed and scale of AI.

Describe Microsoft Copilot for Security terminology

Completed100 XP

- 3 minutes

In this unit, we introduce you to some basic terminology.

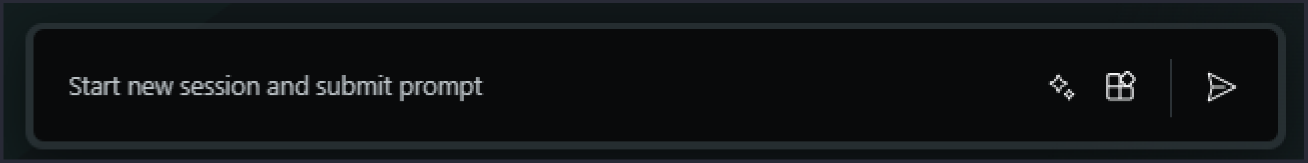
Terminology

The following terms are important for understanding the way Copilot works:

- Session – A particular conversation within Copilot. Copilot maintains context within a session.
- Prompt – A specific statement or question within a session. A user enters a prompt in the prompt bar.
- Capability – A function Copilot uses to solve part of a problem. A capability may sometimes be referred to as a skill.
- Plugin – A collection of capabilities by a particular resource.
- Orchestrator – Copilot's system for composing capabilities together to answer a user's prompt.

Prompt bar and sessions

At the center of Microsoft Copilot for Security is the prompt bar. You use the prompt bar to tell Copilot what insights you want from your security data, this is referred to as the prompt. In other words, the prompt is the text-based, natural language input you provide in the prompt bar that instructs Copilot to generate a response. Although you interact with Copilot in natural language, it's helpful to be specific in the prompts (specific questions or statements) that you provide. For those that are relatively new to the security analyst role and engaging with AI, effective prompting may take some practice. For this reason, Copilot provides promptbooks that provide a series of preselected prompts and prompt suggestions (more details on this in a subsequent module).



As you make requests and as Copilot responds, you may have some follow-up requests. The entirety of the dialog is referred to as a session. Copilot maintains context within a session.

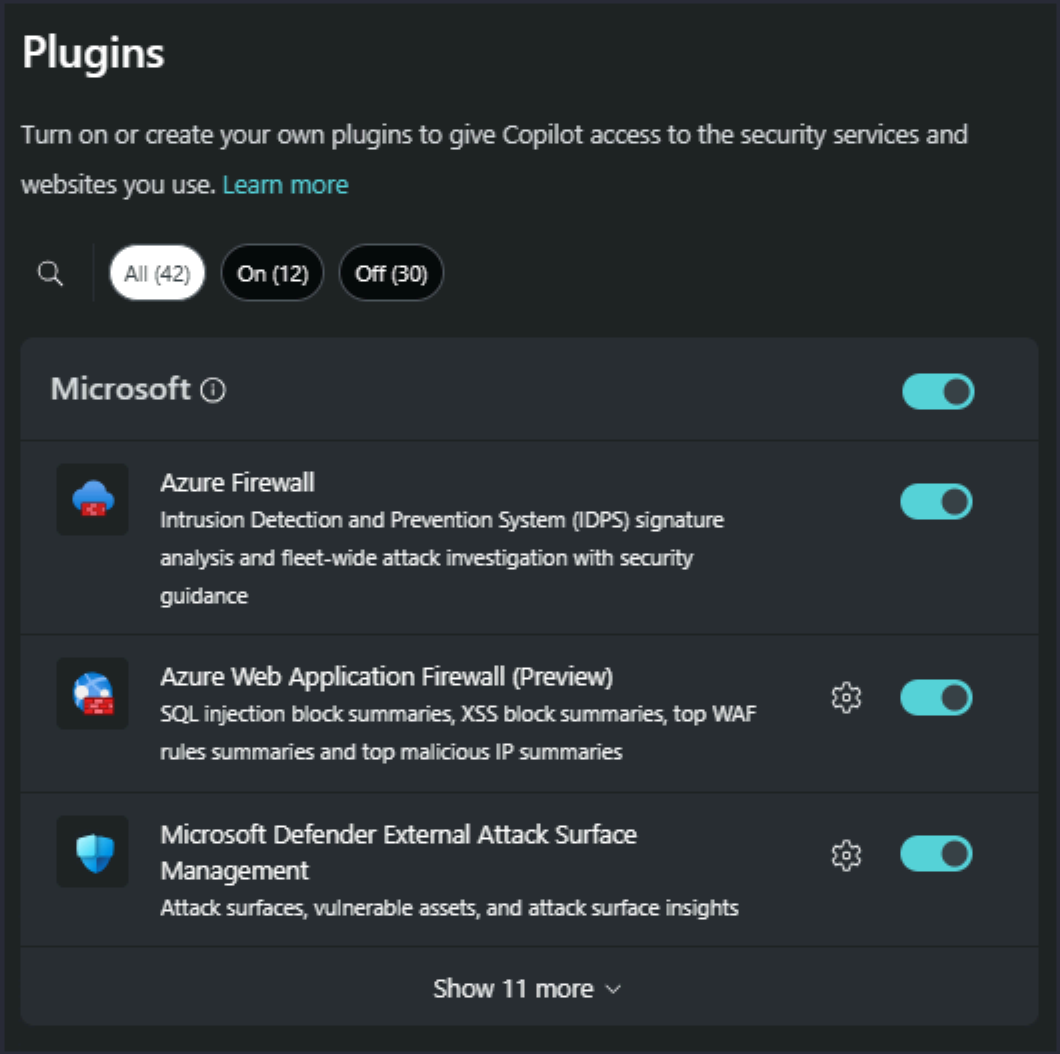
Plugins and capabilities

In the previous unit, we mentioned that Copilot integrates with various sources through plugins, including Microsoft's own security products such as Microsoft Sentinel, Microsoft Defender XDR, and Microsoft Intune, non-Microsoft solutions, and open-source intelligence feeds. The integration enabled by the plugin, for any specific data source, provides Copilot with a collection of capabilities. Each capability is like a function in software, it's designed to do a specialized task within the scope of the data source. For example, the plugin to Microsoft Defender XDR includes a collection of individual capabilities that are used only by Microsoft Defender XDR. These include:

- The ability to summarize an incident.
- Support incident response teams in resolving incidents through guided responses (a set of recommended actions based on the specific incident).
- The ability to analyze scripts and code.
- The ability to generate KQL queries from natural language input.
- The ability to generate incident reports.

A plugin for Microsoft Sentinel may have similar capabilities but runs only within the scope of Microsoft Sentinel.

Copilot currently supports plug-ins for Microsoft services and non-Microsoft services, including websites and custom plug-ins that can be enabled.



Plugins

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

All (42) On (12) Off (30)

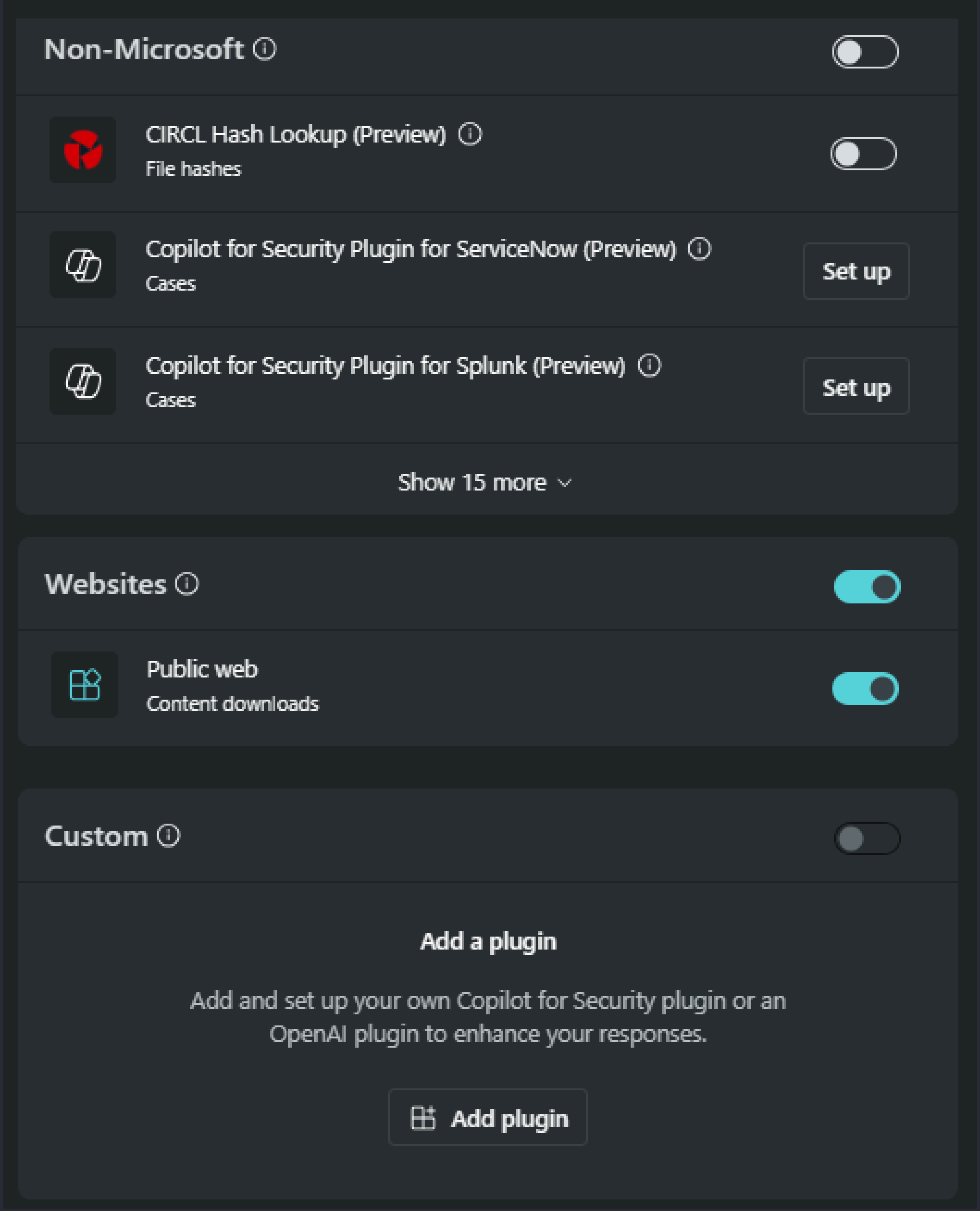
Microsoft ⓘ

Azure Firewall
Intrusion Detection and Prevention System (IDPS) signature analysis and fleet-wide attack investigation with security guidance

Azure Web Application Firewall (Preview)
SQL injection block summaries, XSS block summaries, top WAF rules summaries and top malicious IP summaries

Microsoft Defender External Attack Surface Management
Attack surfaces, vulnerable assets, and attack surface insights

Show 11 more



Non-Microsoft ⓘ

CIRCL Hash Lookup (Preview) ⓘ
File hashes

Copilot for Security Plugin for ServiceNow (Preview) ⓘ
Cases
Set up

Copilot for Security Plugin for Splunk (Preview) ⓘ
Cases
Set up

Show 15 more ⌄

Websites ⓘ

Public web
Content downloads

Custom ⓘ

Add a plugin

Add and set up your own Copilot for Security plugin or an OpenAI plugin to enhance your responses.

Add plugin

Some plugins require setup and configuration, as depicted by the Set up button or the gear icon. For Microsoft plugins, set up may be required where resource specific information needs to be specified. For non-Microsoft sources, set up may be required for account authentication.

Orchestrator

The orchestrator is Copilot’s system for composing capabilities together to answer a user’s prompt. This function is illustrated in more detail in the subsequent unit that describes how Copilot processes prompt requests.

Describe how Microsoft Copilot for Security processes prompt requests

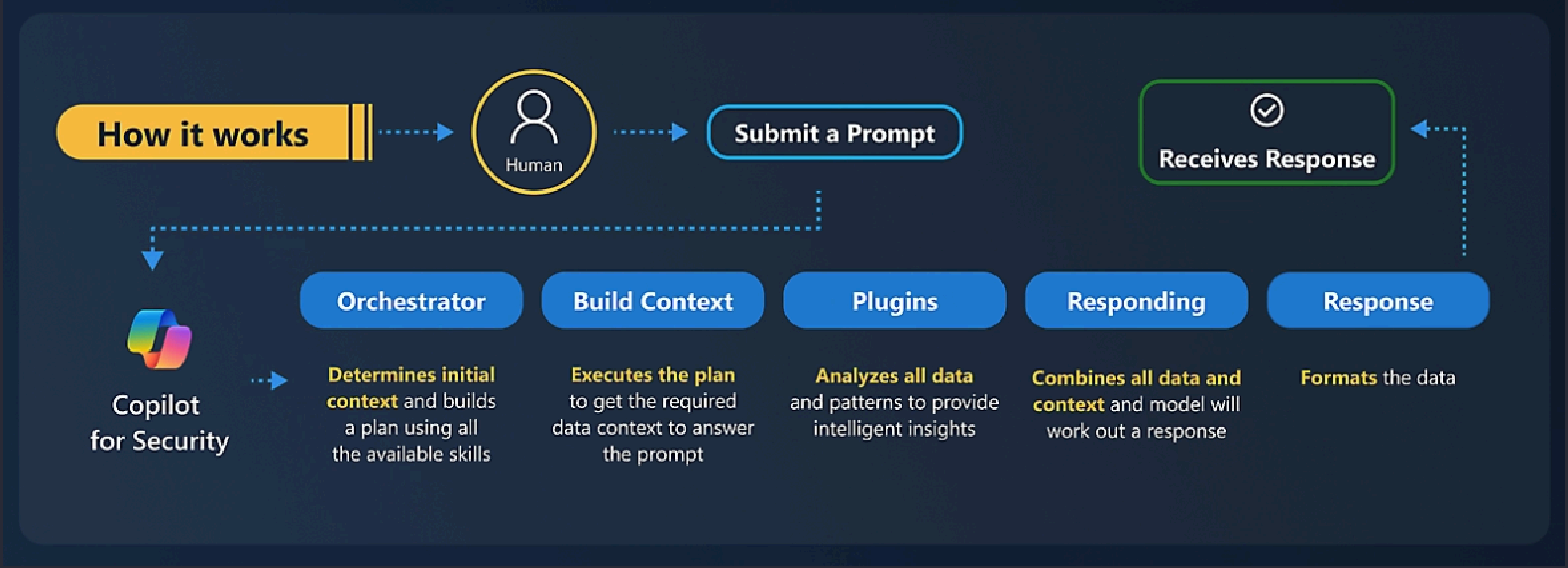
Completed100 XP

- 4 minutes

So now that there's a basic understanding of plugins, capabilities, and how the user interacts with Microsoft Copilot for Security through prompts, it’s worth taking a look under the hood to see how these components come together to process a prompt request and help security analysts.

Process flow

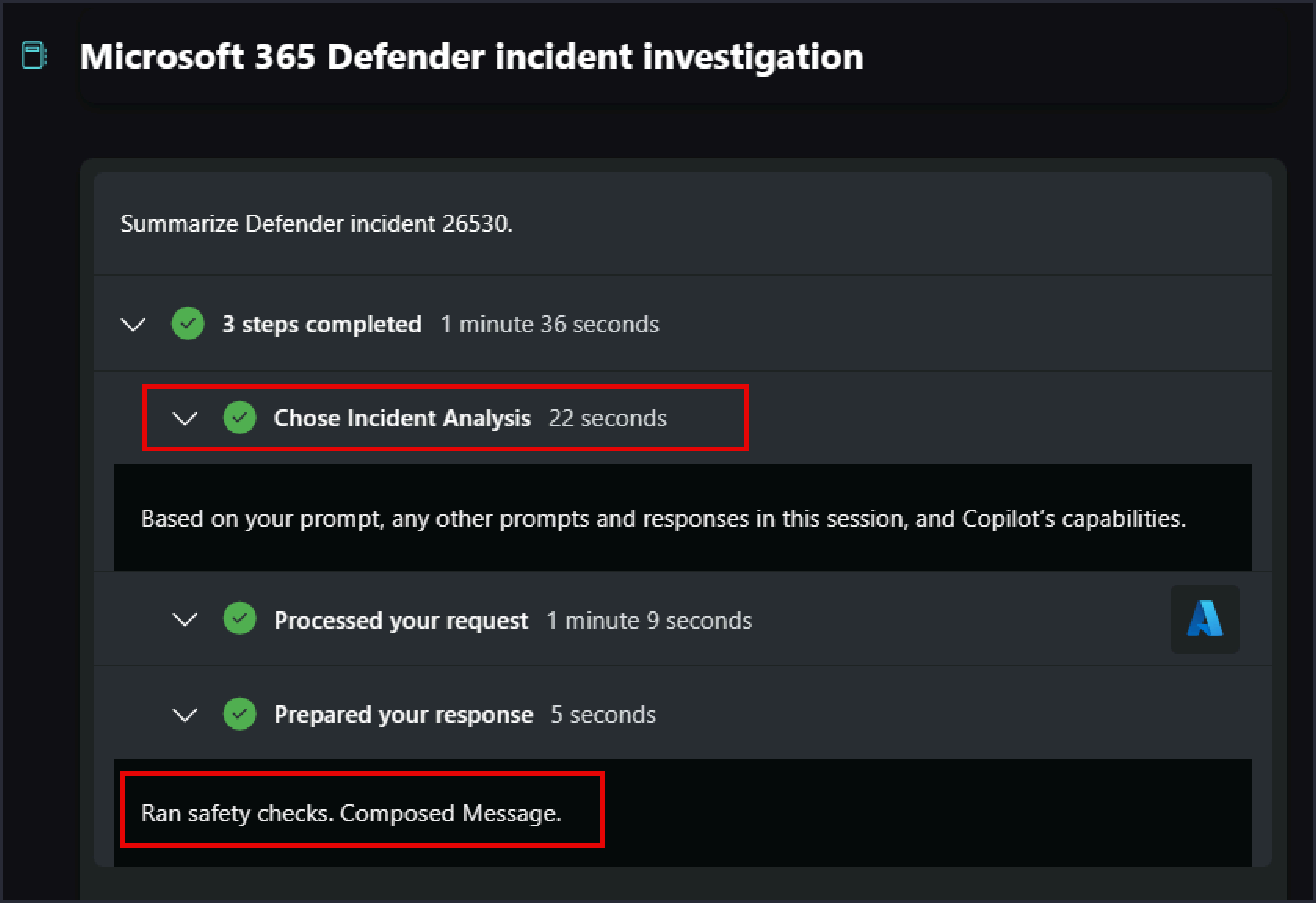
When a user submits a prompt, Copilot processes that prompt to generate the best possible response. The diagram that follows illustrates, at a high level, steps that Copilot takes to process the prompt and generate a response.


How it works
Human
Submit a Prompt
Receives Response
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

1. Submit a prompt: The process starts when a user submits a prompt in the prompt bar.
2. Orchestrator: Copilot for Security sends the information to the Copilot backend referred to as the orchestrator. The orchestrator is Copilot's system for composing capabilities together to answer a user's prompt. It determines the initial context and builds a plan using all the available capabilities (skills).
3. Build context: Once a plan is defined and built, Copilot executes that plan to get the required data context to answer the prompt.
4. Plugins: In the course of executing the plan, Copilot analyzes all data and patterns to provide intelligent insights. This includes reasoning over all the plugins and sources of data, enabled and available to Copilot.
5. Responding: Copilot combines all the data and context and uses the power of its advanced LLM to compose a response using language that makes sense to a human being.
6. Response: Before the response can be sent back to the user, Copilot formats and reviews the response as part of Microsoft's commitment to responsible AI.
7. Receives response: The process culminates with the user receiving the response from the Copilot.

Process log

During this process, Copilot generates a process log that is visible to the user. The user can see what capability is used to generate the response. This is important because it enables the user to determine whether the response was generated from a trusted source. In the screenshot that follows, the process log shows that Copilot chose the Incident Analysis capability. The process log also shows that the final output went through safety checks, which is part of Microsoft's commitment to responsible AI.



Microsoft 365 Defender incident investigation

Summarize Defender incident 26530.

3 steps completed 1 minute 36 seconds

Chose Incident Analysis 22 seconds

Based on your prompt, any other prompts and responses in this session, and Copilot's capabilities.

Processed your request 1 minute 9 seconds

Prepared your response 5 seconds

Ran safety checks. Composed Message.

Describe the elements of an effective prompt

Completed100 XP

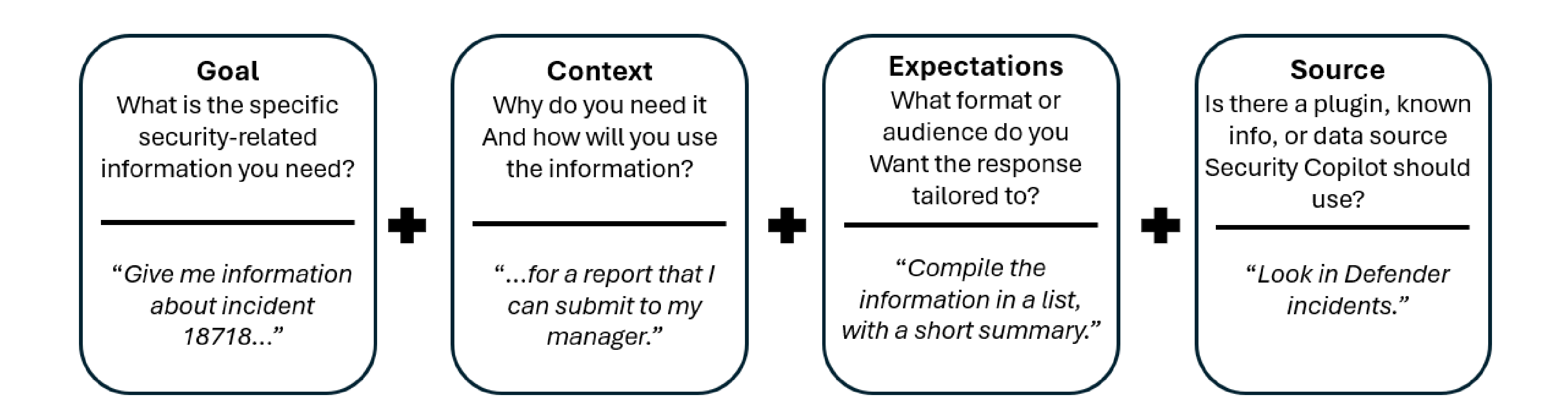
- 4 minutes

In a previous unit, we defined a prompt as the text-based, natural language input you provide in the prompt bar that instructs Microsoft Copilot for Security to generate a response. Copilot provides promptbooks and prompt suggestions, which are helpful, particularly if you're just starting an incident investigation. At some point, however, you'll want and need to enter your own prompts. In those cases, the quality of the response that Copilot returns depends in large part on the quality of the prompt used. In general, a well-crafted prompt with clear and specific inputs leads to more useful responses by Copilot.

Elements of an effective prompt

Effective prompts give Copilot adequate and useful parameters to generate a valuable response. Security analysts or researchers should include the following elements when writing a prompt.

- Goal - specific, security-related information that you need
- Context - why you need this information or how you'll use it
- Expectations - format or target audience you want the response tailored to
- Source - known information, data sources, or plugins Copilot should use



Goal
What is the specific security-related information you need?

"Give me information about incident 18718..."

Context
Why do you need it And how will you use the information?

"...for a report that I can submit to my manager."

Expectations
What format or audience do you Want the response tailored to?

"Compile the information in a list, with a short summary."

Source
Is there a plugin, known info, or data source Security Copilot should use?

"Look in Defender incidents."

Every good prompt should have a goal. Whether it comes in the form of instructions or questions, it should indicate what you want out of your current session.

For Copilot, context can refer to the time frame, or that you'll use the response for a report. Expectations can include whether you want the response to be in a table format, a list of action steps, a summary, or even a diagram. Source might be useful in specifying which Microsoft plugins you're referring to, if needed. Some plugins require more context to work effectively or supporting plugins to ensure a response when initial responses fail.

Watch this short video for a summary on how to create effective prompts.

Other prompting tips

Some things to remember when coming up with your own prompts:

- Be specific, clear, and concise as much as you can about what you want to achieve. You can always start simply with your first prompt, but as you get more familiar with Copilot, include more details following the elements of an effective prompt.
  - Basic prompt: Pearl Sleet actor
  - Better prompt: Can you give me information about Pearl Sleet activity, including a list of known indicators of compromise and tools, tactics, and procedures (TTPs)?
- Iterate. Subsequent prompts are typically needed to further clarify what you need or to try other versions of a prompt to get closer to what you're looking for. Like all LLM-based systems, Copilot can respond to the same prompt in slightly different ways.
- Provide necessary context to narrow down where Copilot looks for data.
  - Basic prompt: Summarize incident 15134.
  - Better prompt: Summarize incident 15134 in Microsoft Defender XDR into a paragraph that I can submit to my manager and create a list of entities involved.
- Give positive instructions instead of "what not to do." Copilot is geared toward action, so telling it what you want it to do for exceptions is more productive.
  - Basic prompt: Give me a list of unmanaged devices in my network.
  - Better prompt: Give me a list of high-risk unmanaged devices in my network. If they're named "test" remove them from the list.
- Directly address Copilot as "You" as in, "You should ..." or "You must ...", as this is more effective than referring to it as a model or assistant.

While these guidelines can help you get started in creating prompts, it’s important to note that you’re not limited to forming prompts following the structure of the previous examples. What’s great about Copilot is that it's designed to respond to questions or instructions made in your own words (that is, using natural language).

You have the flexibility to adapt these guidelines to your specific needs.

Describe how to enable Microsoft Copilot for Security

Completed100 XP

- 5 minutes

To start using Microsoft Copilot for Security, organizations need to take steps to onboard the service and users. These include:

1. Provision Copilot capacity
2. Set up the default environment
3. Assign role permissions

Provision capacity

Microsoft Copilot for Security is sold as a consumptive offering, meaning that customers are billed monthly based on a provisioned capacity that is billed by the hour. The capacity that is provisioned is referred to as a security compute unit (SCU). An SCU is the unit of measure of computing power used to run Copilot in both the standalone and embedded experiences.

Before users can start using Copilot, admins need to provision and allocate capacity. To provision capacity:

- You must have an Azure subscription.
- You need to be an Azure owner or Azure contributor, at a resource group level, as a minimum. *Keep in mind that a global administrator in Microsoft Entra ID doesn't necessarily have the Azure owner or Azure contributor role by default. Microsoft Entra role assignments don't grant access to Azure resources. As a global admin in Entra, you can enable access management for Azure resources through the Azure portal. For details, see Elevate access to manage all Azure subscriptions and management groups. Once you've enabled access management to Azure resources, you can configure the appropriate Azure role.*

There are two options for provisioning capacity:

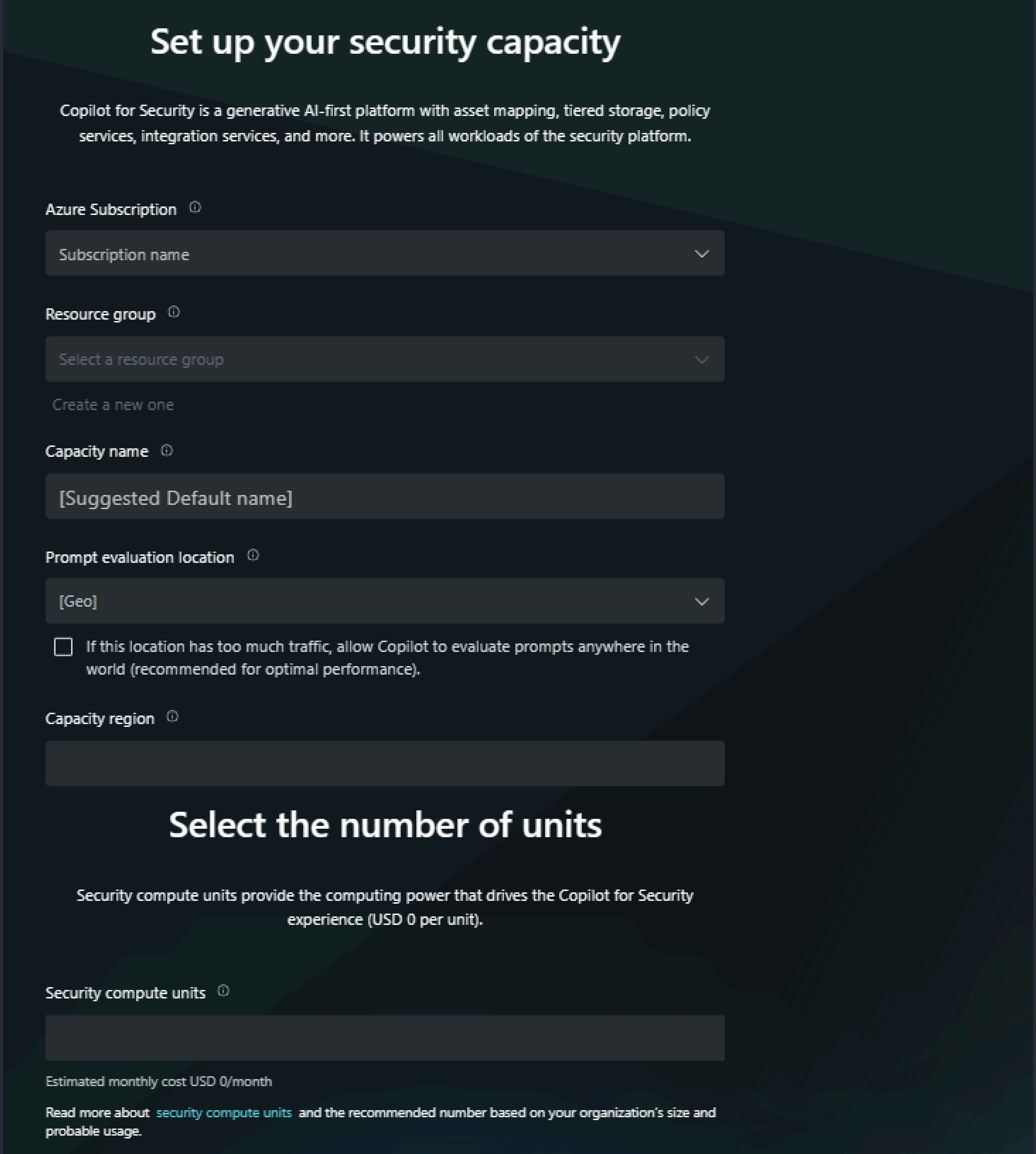
- Provision capacity within Copilot for Security (recommended)

- Provision capacity through Azure

Note

Regardless of the method you choose, you will need to purchase a minimum of 1 and a maximum of 100 SCUs.

Provision capacity within Copilot for Security. When you first open Copilot for Security as an admin, a wizard guides you through the steps in setting up capacity for your organization. The wizard prompts you for information including your Azure subscription, resource group, region, capacity name, and the quantity of SCUs.



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

Subscription name

Resource group

Select a resource group

Create a new one

Capacity name

[Suggested Default name]

Prompt evaluation location

[Geo]

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

Capacity region

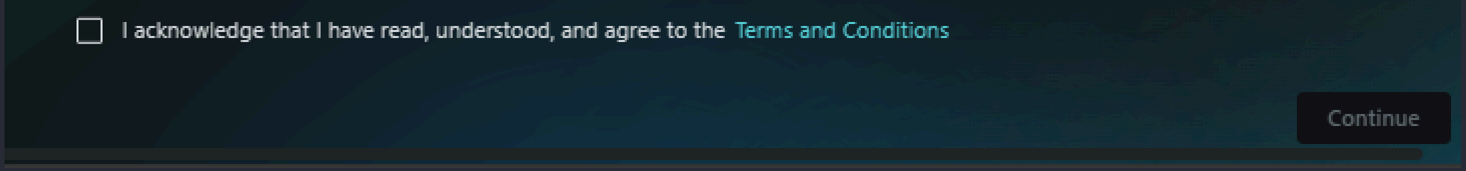
Select the number of units

Security compute units provide the computing power that drives the Copilot for Security experience (USD 0 per unit).

Security compute units

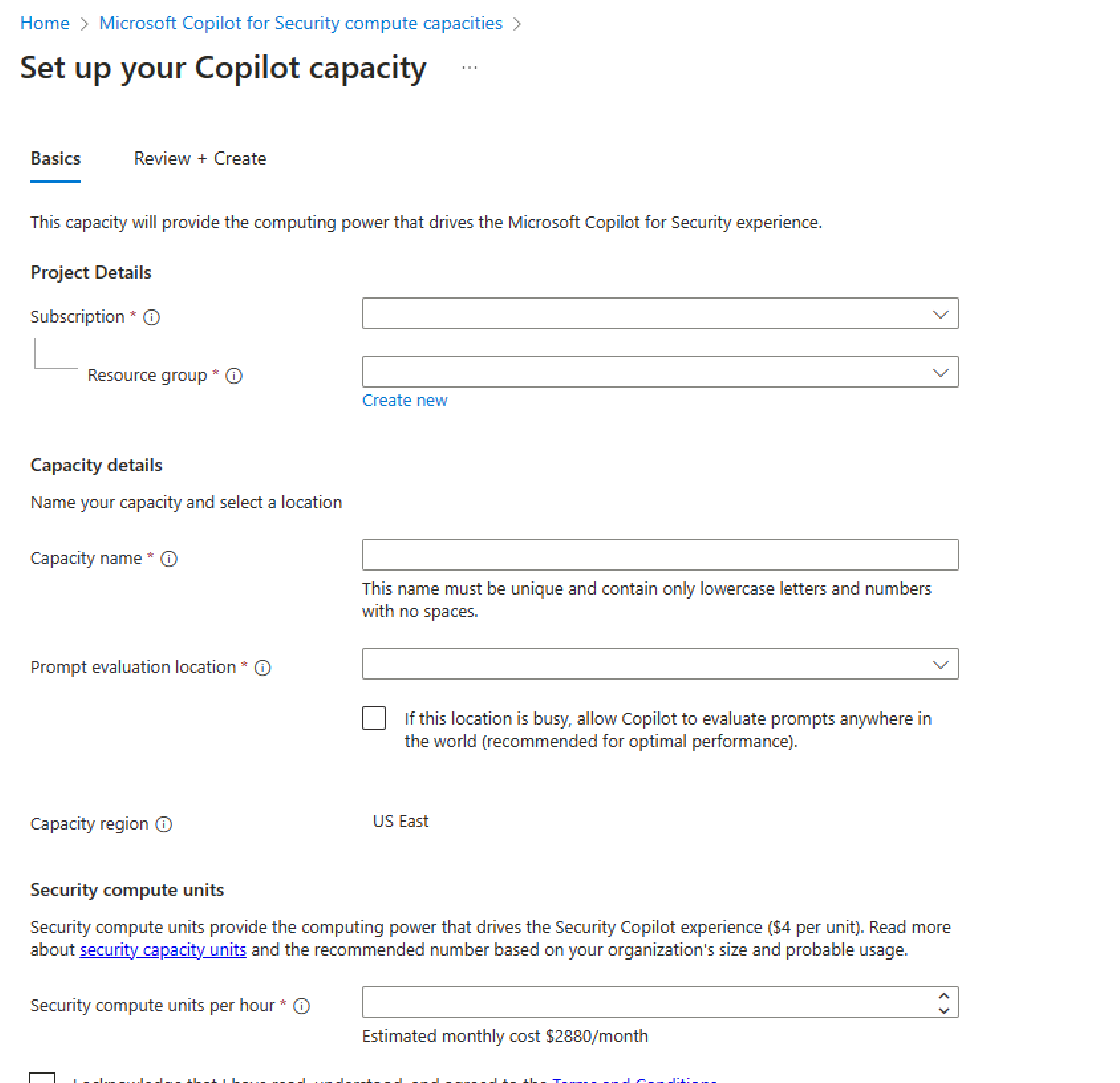
Estimated monthly cost USD 0/month

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

Provision capacity through Azure. The Azure portal now includes Copilot for Security as a service. Selecting the service, opens the page where you input information including your Azure subscription, resource group, region, capacity name, and the quantity of SCUs.



Home > Microsoft Copilot for Security compute capacities >

Set up your Copilot capacity ···

Basics | Review + Create

This capacity will provide the computing power that drives the Microsoft Copilot for Security experience.

Project Details

Subscription * ⓘ

Resource group * ⓘ

Create new

Capacity details

Name your capacity and select a location

Capacity name * ⓘ

This name must be unique and contain only lowercase letters and numbers with no spaces.

Prompt evaluation location * ⓘ

□ If this location is busy, allow Copilot to evaluate prompts anywhere in the world (recommended for optimal performance).

Capacity region ⓘ US East

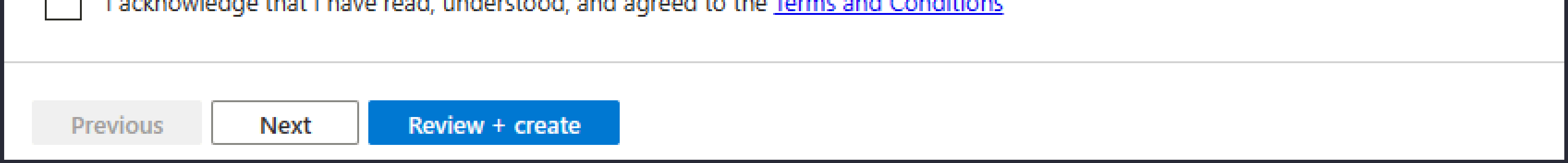
Security compute units

Security compute units provide the computing power that drives the Security Copilot experience ($4 per unit). Read more about security capacity units and the recommended number based on your organization's size and probable usage.

Security compute units per hour * ⓘ

Estimated monthly cost $2880/month

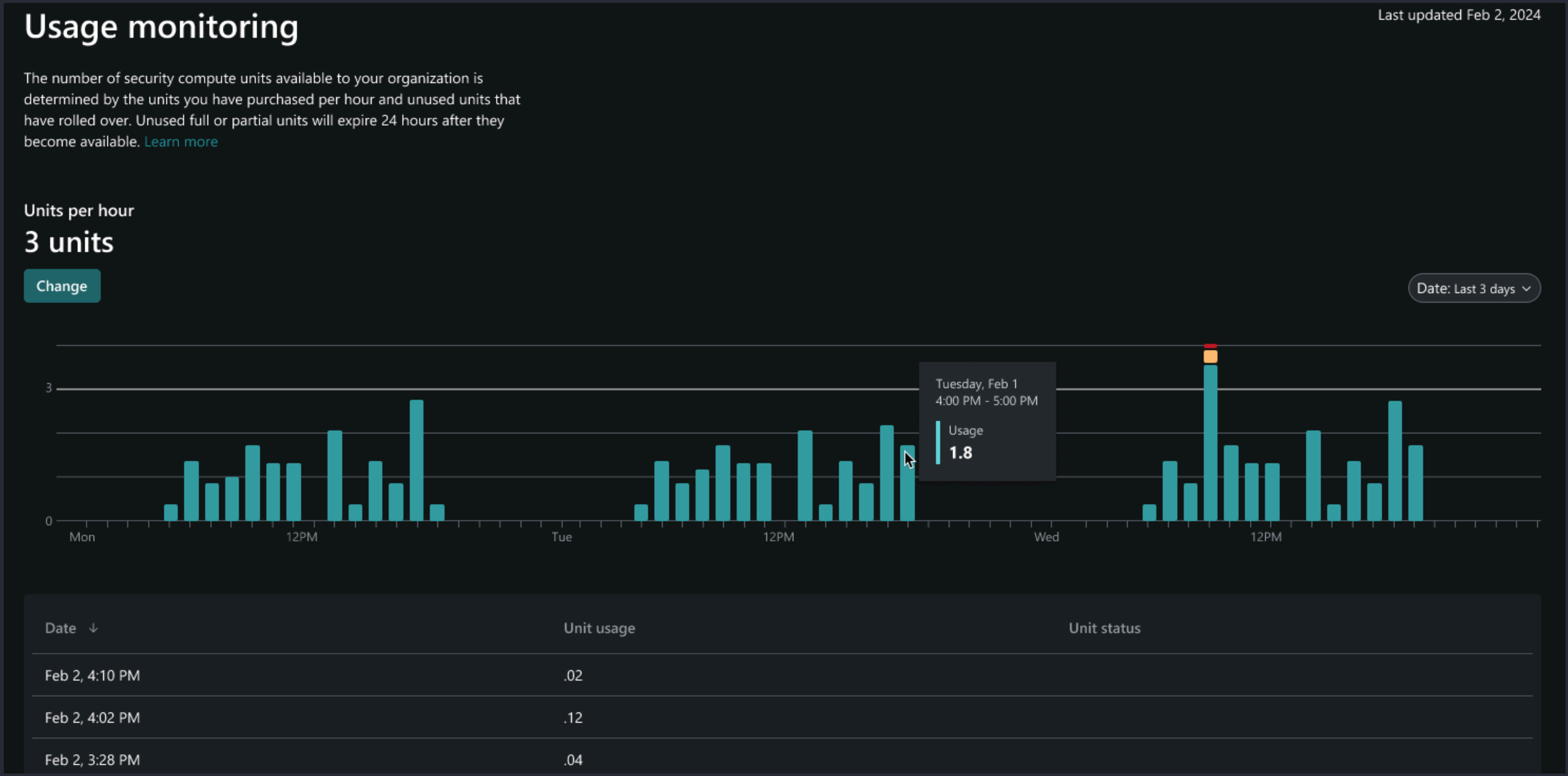
□ I acknowledge that I have read, understood, and agreed to the Terms and Conditions



□ I acknowledge that I have read, understood, and agreed to the Terms and Conditions

Regardless of the approach you choose to provision capacity, the process takes the information and establishes a resource group for the Microsoft Copilot for Security service, within your Azure subscription. The SCUs are an Azure resource within that resource group. Deployment of the Azure resource can take a few minutes.

Once admins complete the steps to onboard to Copilot, they can manage capacity by increasing or decreasing provisioned SCUs within the Azure portal or the Microsoft Copilot for Security product itself. Copilot for Security provides a usage monitoring dashboard for capacity owners allowing them to track usage over time and make informed decisions about capacity provisioning.



Usage monitoring

Last updated Feb 2, 2024

The number of security compute units available to your organization is determined by the units you have purchased per hour and unused units that have rolled over. Unused full or partial units will expire 24 hours after they become available. Learn more

Units per hour
3 units

Date ↓	Unit usage	Unit status
Feb 2, 4:10 PM	.02	
Feb 2, 4:02 PM	.12	
Feb 2, 3:28 PM	.04	

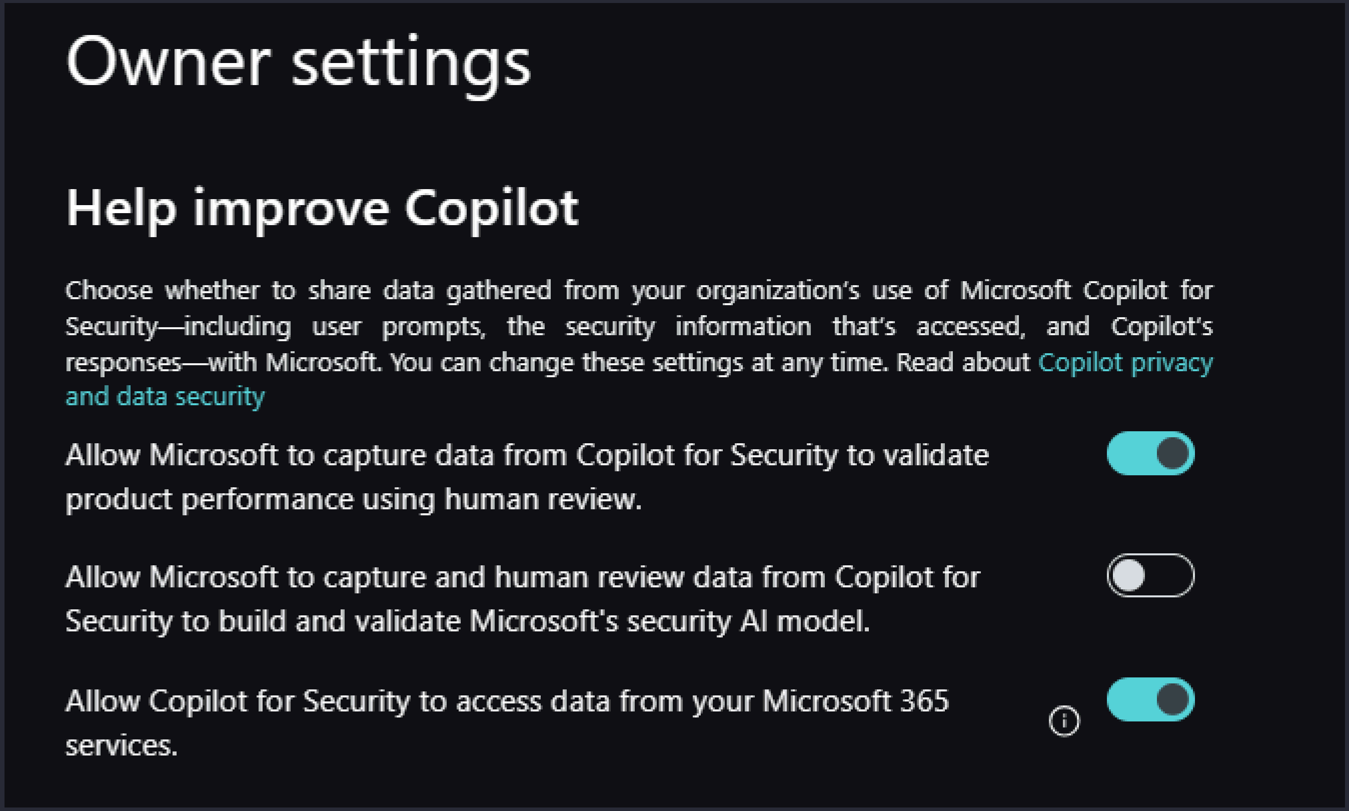
Set up the default environment

To set up the default environment, you need to have one of the following Microsoft Entra ID roles:

- Global administrator
- Security administrator

During the setup of Copilot for Security, you're prompted to configure settings. These include:

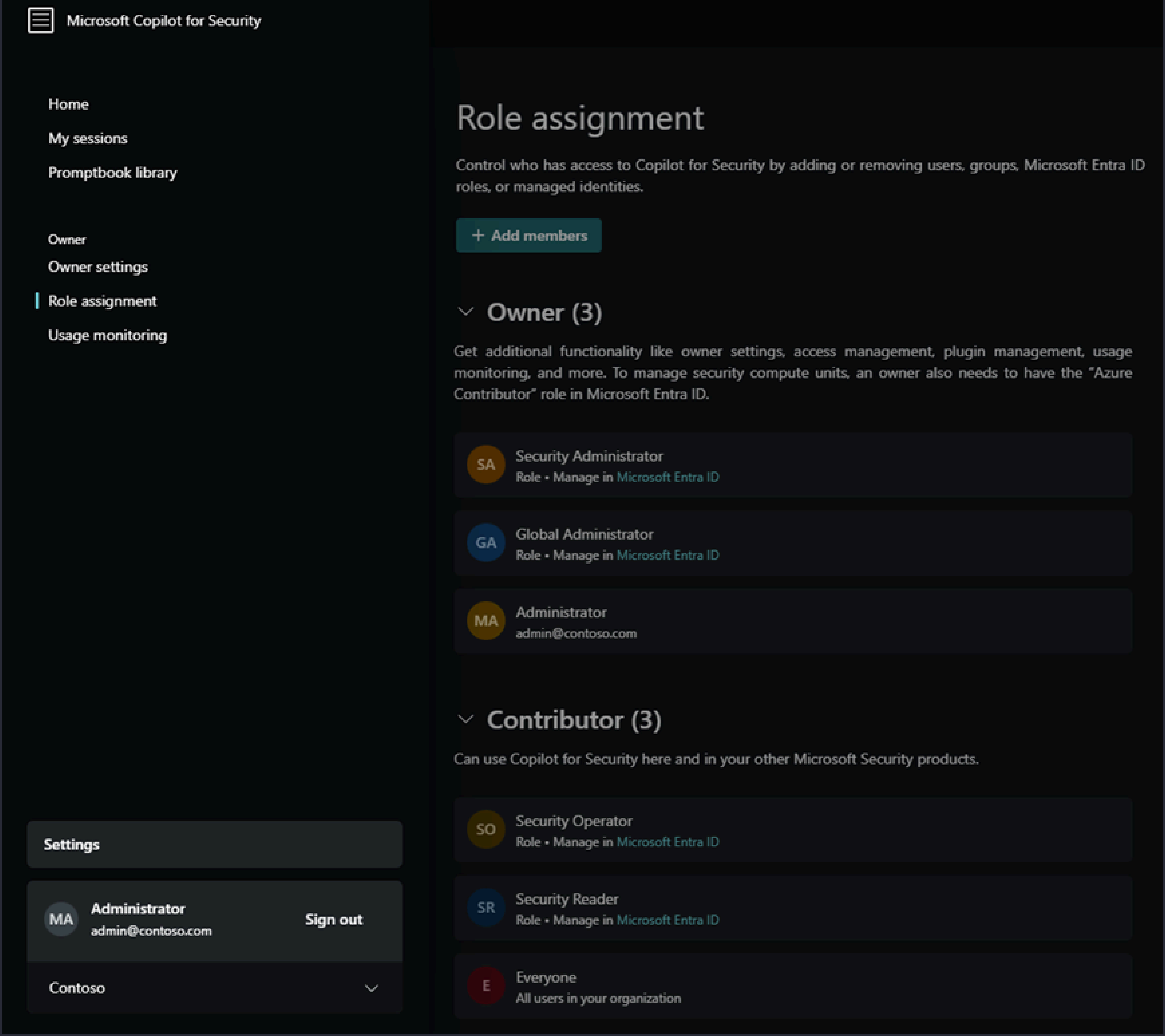
- SCU capacity - Select the capacity of SCUs previously provisioned.
- Data storage - When an organization onboards to Copilot, the admin must confirm the geographic location of the tenant as the customer data collected by the services is stored there. Microsoft Copilot for Security operates in the Microsoft Azure data centers in the European Union (EUDB), the United Kingdom, the United States, Australia and New Zealand, Japan, Canada, and South America.
- Your organization's data - The admin must also opt in or opt out of data sharing options. Turn the toggles on or off for any of the following options:
    - Allow Microsoft to capture data from Copilot for Security to validate product performance using human review: When turned on, customer data is shared with Microsoft for product improvement. Prompts and responses are evaluated to understand whether the right plugins were selected, if the output is what was expected, how responses, latency, and output format can be improved.
    - Allow Microsoft to capture and human review data from Copilot for Security to build and validate Microsoft's security AI model: When turned on, customer data is shared with Microsoft for Copilot AI improvement. Opting in does NOT allow Microsoft to use customer data to train foundational models. Prompts and responses are evaluated to enhance responses and to ensure they're what's expected and useful to you.
    - Allow Copilot for Security to access data from your Microsoft 365 services. If this option is turned off, your organization won't be able to use plugins that access Microsoft 365 services. Currently, this option is required for use of the Microsoft Purview plugin. Setting and/or changing this setting requires a user with a Global administrator role. For more information

> about how Microsoft handles your data, see *Data security and privacy*.
>
> 
>
> # Owner settings
>
> ## 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. ⓘ ●

- Decide where your prompts are evaluated - You can restrict the evaluation within your geo or allow evaluation anywhere in the world. For more information on the list of mapped locations for your geo, see Data security and privacy.
- Roles - You're informed of the required roles that need to be assigned for users in your organization to use Copilot for Security.

Role permissions

To ensure that the users can access the features of Copilot, they need to have the appropriate role permissions.



Administrator
admin@contoso.com

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

Permissions can be assigned using Microsoft Entra ID roles or Copilot for Security roles. As a best practice, provide the least privileged role applicable for each user.

The Microsoft Entra ID roles are:

- Global administrator
- Security administrator
- Security operator
- Security reader

Although these roles grant users varying levels of access to Copilot, the scope of these roles extends beyond Copilot. For this reason, Copilot for Security introduces two roles that function like access groups but aren't Microsoft Entra ID roles. Instead, they only control access to the capabilities of the Copilot for Security platform.

The Microsoft Copilot for Security roles are:

- Copilot owner
- Copilot contributor

The Security Administrator and Global Administrator roles in Microsoft Entra automatically inherit Copilot owner access.

By default, all users in the Microsoft Entra tenant are given Copilot contributor access.

- Any user within a licensed tenant (purchased Copilot via the consumption model) will be allowed to create a session/prompt by default.
- If the admin doesn't wish to provide access to everyone in the licensed tenant to be able to run prompts, they can restrict access to run prompts by removing “All users” from the Workspace Contributor Role assignments and adding an existing security group from the Copilot for Security portal.
- All experiences where Copilot for Security is used (embedded or standalone) will follow the updates made by the admin.
- Admin/Owner permissions are required for any privileged operations like associating the workspace to SCU capacity, owner settings, plugin settings, and more.
- Provisioning Capacity operations continue to require Azure owner or Azure contributor roles, enabled through Azure IAM.

For a detailed listing of the permissions granted for each of these roles, refer to the Assign roles section in *Understand authentication in Microsoft Copilot for Security*.

Your role controls what activities you have access to, such as configuring settings, assigning permissions, or performing tasks. Copilot doesn't go beyond the access you have. Additionally, individual Microsoft plugins may have their own role requirements for accessing the service and data it represents. As an example, an analyst that has been assigned a security operator role or a Copilot workspace contributor role is able to access the Copilot portal and create sessions, but to utilize the Microsoft Sentinel plugin would need an appropriate role like Microsoft Sentinel Reader to access incidents in the workspace. To access the devices, privileges, and policies available through the Microsoft Intune plugin, that same analyst would need another service-specific role like the Intune Endpoint Security Manager role.

Generally speaking, Microsoft plugins in Copilot use the OBO (on behalf of) model – meaning that Copilot knows that a customer has licenses to specific products and is automatically signed into those products. Copilot can then access the specific products when the plugin is enabled and, where applicable, parameters are configured. Some Microsoft plugins that require setup may include configurable parameters that are used for authentication in-lieu of the OBO model.

Summary and resources

Completed100 XP

- 1 minute

Microsoft Copilot for Security is an AI-powered, cloud-based security analysis tool designed to help organizations meet the growing challenges of cybersecurity, such as increasing attack sophistication and a shortage of skilled personnel. It enables security analysts to respond to threats at machine speed, process signals rapidly, and assess risk exposure more efficiently than traditional methods. Copilot is a comprehensive solution for managing security posture, responding to incidents, and generating actionable security reports.

Copilot offers a user-friendly interface, allowing interactions through natural language prompts. It integrates seamlessly with Microsoft security products like Microsoft Defender XDR and Microsoft Sentinel and also with non-Microsoft solutions, through plugins, providing a unified view for security analysis. The use of OpenAI's natural language processing models enhances its capability to understand and process user requests, making it an effective tool for both seasoned and novice security analysts.

Copilot maintains high standards of data privacy and security. The process log feature further adds transparency, allowing users to track the source and validity of the information provided by the tool.

Now that you've completed this module, you should be able to:

- Describe what Microsoft Copilot for Security is.
- Describe the terminology of Microsoft Copilot for Security.
- Describe how Microsoft Copilot for Security processes prompt requests.
- Describe the elements of an effective prompt
- Describe how to enable Microsoft Copilot for Security.