

Explore Use Cases of Microsoft Copilot for Security

Explore use cases of Microsoft Copilot for Security

- 2 hr 19 min
- Module
- 11 Units

Feedback

Beginner

Security Engineer

Security Operations Analyst

Business Owner

Microsoft Copilot

Microsoft Defender XDR

Microsoft Purview

Explore use cases of Microsoft Copilot for Security in the standalone and embedded experiences, through lab-like exercises.

Learning objectives

By the end of this module, you'll be able to:

- "Set up Microsoft Copilot for Security."
- "Work with sources in Copilot."
- "Create a custom promptbook."

- "Use the capabilities of Copilot in Defender XDR."
- "Use the capabilities of Copilot in Microsoft Purview."

StartAdd

Prerequisites

- Working knowledge of security operations and incident response
- Working knowledge of Microsoft Security solutions and services
- Completion of the module [Describe Microsoft Copilot for Security](#)
- Completion of the module [Describe the core features of Microsoft Copilot for Security](#)
- Completion of the module [Describe the embedded experiences of Microsoft Copilot for Security](#)

This module is part of these learning paths

- [Get started with Microsoft Copilot for Security](#)
- [SC-200: Mitigate threats using Microsoft Copilot for Security](#)

Introduction

Completed100 XP

- 1 minute

This module guides you through a series of simulation-based exercises that mimic real-world situations, helping you understand how to effectively use Microsoft Copilot for Security in your own work environment.

The exercises covered in this module include:

- Setting Up and provisioning Microsoft Copilot for Security.
- Exploring the standalone experience of Microsoft Copilot for Security.

- Managing sources.
 - Working with prompts and promptbooks.
 - Exploring the features of the different embedded experiences.
-

Explore the first run experience

Completed100 XP

- 15 minutes

The organization you work for wants to increase the efficiency and capabilities of its security analyst to improve security outcomes. In support of that objective, the office of the CISO determined that deploying Microsoft Copilot for Security is a key step towards that objective. As the Security administrator for your organization, you're tasked with setting up Copilot.

In this exercise, you go through the first run experience of Microsoft Copilot for Security to provision Copilot with one security compute unit (SCU).

Note

The environment for this exercise is a simulation generated from the product. As a limited simulation, links on a page may not be enabled and text-based inputs that fall outside of the specified script may not be supported. A pop-up message will display stating, "This feature is not available within the simulation." When this occurs, select OK and continue the exercise steps.

81lh1gioqh-w1c003zuj7.app.highlights.guide says

This feature is not available within the simulation.

OK

Exercise

For this exercise, you're logged in as Avery Howard and you have the global administrator role in Microsoft Entra. You'll work in both the Azure portal and Microsoft Copilot for Security.

This exercise should take approximately **15** minutes to complete.

Note

When a lab instruction calls for opening a link to the simulated environment, it is generally recommended that you open the link in a new browser window so that you can simultaneously view the instructions and the exercise environment. To do so, select the right mouse key and select the option.

Task: Set role permissions

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.

In this task, you walk through the process of ensuring you have the appropriate role permissions. This starts by enabling access management for Azure resources.

Why is this needed? As a Global Administrator in Microsoft Entra ID, you might not have access to all subscriptions and management groups in your directory. Microsoft Entra ID and Azure resources are secured independently from one another. That is, Microsoft Entra role assignments don't grant access to Azure resources, and Azure role assignments don't grant access to Microsoft Entra ID. When you elevate your access, you're assigned the User Access Administrator role in Azure at root scope (/). This allows you to view all resources and assign access in any subscription or management group in the directory. For details, see [Elevate access to manage all Azure subscriptions and management groups](#).

Once you're assigned the User Access Administrator role in Azure, you can assign a user the necessary access to provision SCUs for Copilot. For the purpose of this exercise only, which is to show you the steps involved, you will be assigning yourself the necessary access. The steps that follow will guide you through the process.

1. Open the simulated environment by selecting this link: [Azure portal](#).
2. You'll start by enabling Access management for Azure resources. To access this setting:
 1. From the Azure portal, select **Microsoft Entra ID**.
 2. From the left navigation panel, expand **Manage**.
 3. From the left navigation panel, scroll down and select **Properties**.
 4. Enable the toggle switch for **Access management for Azure resources**, then select **Save**.

3. Now that you can view all resources and assign access in any subscription or management group in the directory, assign yourself the Owner role for the Azure subscription.
 1. From the blue banner on the top of the page, select **Microsoft Azure** to return to the landing page of the Azure portal.
 2. Select **Subscriptions** then select the subscription listed **Woodgrove - GTP Demos (External/Sponsored)**.
 3. Select **Access control (IAM)**.
 4. Select **Add**, then **Add role assignment**.
 5. From the Role tab, select **Privileged administrator roles**.
 6. Select **Owner**, then select **Next**.
 7. Select **+ Select members**.
 8. Avery Howard is the first name on this list, select the **+** to the right of the name. Avery Howard is now listed under selected members. Select the **Select** button, then select **Next**.
 9. Select **Allow user to assign all roles except privileged administrator roles, Owner, UAA, RBAC (Recommended)**.
 10. Select **Review + assign**, then select **Review + assign** one last time.

As an owner to the Azure subscription, you'll now be able to provision capacity within Copilot.

Task: Provision capacity

In this task, you go through the steps of provisioning capacity for your organization. There are two options for provisioning capacity:

- Provision capacity within Copilot for Security (recommended)
- Provision capacity through Azure

For this exercise, you provision capacity through Copilot for Security. When you first open Copilot for Security, a wizard guides you through the steps in setting up capacity for your organization.

1. Open the simulated environment by selecting this link: **Microsoft Copilot for Security**.
2. Follow the steps in the Wizard, select **Get started**.
3. On this page, you set up your security capacity. For any of the fields listed below, you can select the information icon for more information.
 1. Azure subscription: From the drop-down, select **Woodgrove - GTP Demos (External/Sponsored)**.
 2. Resource group: From the drop-down, select **RG-1**.

3. Capacity name: Enter a capacity name.
4. Prompt evaluation location [Geo]: From the drop-down, select your region.
5. You can choose whether you want to select the option, "If this location has too much traffic, allow Copilot to evaluate prompts anywhere in the world (recommended for optimal performance).
6. Capacity region is set based on location selected.
7. Security compute: This field is automatically populated with the minimum required SCU units, which is 1. Leave field with the value of **1**.
8. Select the box, **"I acknowledge that I have read, understood, and agree to the Terms and Conditions"**.
9. Select **Continue** on the bottom right corner of the page.
4. The wizard displays information about where your customer data will be stored. The region displayed is based on the region you selected in the Prompt evaluation field. Select **Continue**.
5. You can select options to help improve Copilot. You can select the toggle based on your preferences. Select **Continue**.
6. As part of the initial setup, Copilot provides contributor access to everyone by default and includes Global administrators and Security administrators as Copilot owners. In your production environment, you can change who has access to Copilot, once you've completed the initial setup. Select **Continue**.
7. You're all set! Select **Finish**.
8. Close the browser tab, as the next exercise will use a separate link to the lab-like environment.

Review

In this exercise, you successfully provisioned Copilot for Security. You're now ready to move to the next exercise where you'll explore the core functionality of Microsoft Copilot for Security.

Explore the standalone experience

Completed 100 XP

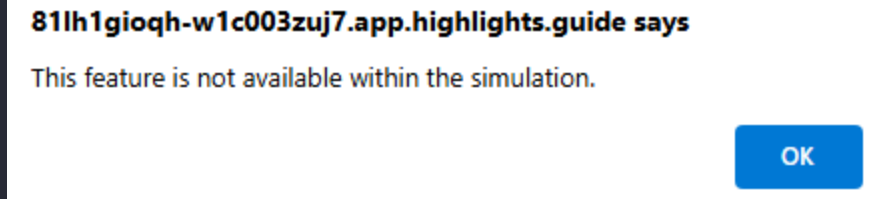
- 15 minutes

The security administrator for your organization provisioned Copilot. Since you're the senior analyst on the team, the administrator added you as a Copilot owner and asked you to familiarize yourself with the solution.

In this exercise, you explore all the key landmarks in the landing page of the standalone experience of Microsoft Copilot for Security.

Note

The environment for this exercise is a simulation generated from the product. As a limited simulation, links on a page may not be enabled and text-based inputs that fall outside of the specified script may not be supported. A pop-up message will display stating, "This feature is not available within the simulation." When this occurs, select OK and continue the exercise steps.



Exercise

For this exercise, you're logged in as Avery Howard and have the Copilot owner role. You'll work in the standalone experience of Microsoft Copilot for Security.

This exercise should take approximately **15** minutes to complete.


Note

When a lab instruction calls for opening a link to the simulated environment, it is generally recommended that you open the link in a new browser window so that you can simultaneously view the instructions and the exercise environment. To do so, select the right mouse key and select the option.

Task: Explore the menu options

In this task, you start your exploration in the home menu.

1. Open the simulated environment by selecting this link: [Microsoft Copilot for Security](#).

2. Select the **Menu** icon  , which is sometimes referred to as the hamburger icon.
3. Select **My sessions** and note the available options.
 1. Select recent to view the most recent sessions
 2. Select filter and note the available options, then close the filter.
 3. Select the home menu icon to open the home menu.
4. Select **Promptbook library**.
 1. Select My promptbooks. A subsequent task dives deeper into promptbooks.
 2. Select Woodgrove.
 3. Select Microsoft.
 4. Select filter to view the available options, then select the X to close.
 5. Select the home menu icon to open the home menu.
5. Select **Owner settings**. These settings are available to you as a Copilot owner. A Copilot contributor does not have access to these menu options.
 1. For plugins for Copilot for Security, select the drop-down for Who can add and manage their own custom plugins to view the available options.
 2. Select drop-down for Who can add and manage custom plugins for everyone in the organization to view the available options. Note, this option is greyed out if Who can add and manage their own custom plugins is set to owners only.
 3. Select the information icon next to "Allow Copilot for Security to access data from your Microsoft 365 Services." This setting must be enabled if you want to use the Microsoft Purview plugin. You'll work with this setting in a later exercise.
 4. Select the drop-down for who can upload files to view the available options.
 5. Select the home menu icon to open the home menu.
6. Select **Role assignment**.
 1. Select Add members, then close.
 2. Expand owner.
 3. Expand contributor.
 4. Select the home menu icon to open the home menu.
7. Select **Usage monitoring**.
 1. Select the date filter to view available options.
 2. Select the home menu icon to open the home menu.

8. Select **Settings**.
 1. Select preferences. Scroll down to view available options.
 2. Select data and privacy.
 3. Select About.
 4. Select the X to close the preferences window.
9. Select where it says **Woodgrove** at the bottom left of the home menu.
 1. When you select this option, you see your tenants. This is referred to as the tenant switcher. In this case, Woodgrove is the only available tenant.
 2. Select the **Home** to return to the landing page.

Task: Explore access to recent sessions

In the center of the landing page, there are cards representing your most recent sessions.

1. The largest card is your last session. Selecting the title of any session card takes you to that session.
2. Select **View all sessions** to go to the My sessions page.
3. Select **Microsoft Copilot for Security**, next to the home menu icon, to return to the landing page.

Task: Explore access to promptbooks

The next section of the Copilot landing page revolves around promptbooks. The landing page shows tiles for some Microsoft security promptbooks. Here you explore access to promptbooks and the promptbook library. In a subsequent exercise, you explore creating and running a promptbook.

1. To the right of where it says "Get started with these promptbooks" are a left and right arrow key that allows you to scroll through the tiles for Microsoft security promptbooks. Select the **right arrow >**
2. Each tile shows the title of the promptbook, a brief description, the number of prompts, and a run icon. Select the title of any of the promptbook tiles to open that promptbook. Select **Vulnerability impact assessment**, as an example.
 1. The window for the selected promptbook provides information, including who created the promptbook, tags, a brief description, inputs required to run the promptbook, and a listing of the prompts.
 2. Note the information about the promptbook and the available options. For this simulation you can't start a new session, you'll do that in a subsequent exercise.

3. Select **X** to close the window.
3. Select **View the promptbook library**.
 1. To view promptbooks that you own, select My promptbooks.
 2. Select Woodgrove for a listing of promptbooks owned by Woodgrove, the name of a fictitious organization.
 3. To view built-in, Microsoft owned/developed promptbooks, select Microsoft.
 4. Select the filter icon. Here you can filter based on tags assigned to the workbook. Close the filter window by selecting the X in the New filter tab.
 5. Select **Microsoft Copilot for Security**, next to the home menu icon, to return to the landing page.

Task: Explore the prompts and sources icon in the prompt bar

At the bottom center of the page is the prompt bar. The prompt bar includes the prompts and sources icon, which you explore in this task. In subsequent exercises you'll enter inputs directly in the prompt bar.

1. From the prompt bar, you can select the prompts icon to select a built-in prompt or a promptbook. Select the **prompts icon**



1. Select **See all promptbooks**
 1. Scroll to view all the available promptbooks.
 2. Select the **back-arrow** next to the search bar to go back.
2. Select **See all system capabilities**. The list shows all available system capabilities (these capabilities are in effect prompts that you can run). Many system capabilities are associated with specific plugins and as such will only be listed if the corresponding plugin is enabled.
 1. Scroll to view all the available promptbooks.
 2. Select the **back-arrow** next to the search bar to go back.

2. Select the **sources icon**



1. The sources icon opens the manage sources window. From here, you can access Plugins or Files. The **Plugins** tab is selected by default.
 1. Select whether you want to view all plugins, those that are enabled (on), or those that are disabled (off).
 2. Expand/collapse list of Microsoft, non-Microsoft, and custom plugins.

3. Some plugins require configuring parameters. Select the **Set up** button for the Microsoft Sentinel plugin, to view the settings window. Select **cancel** to close the settings window. In a separate exercise, you configure the plugin.
2. You should still be in the Manage sources window. Select **Files**.
 1. Review the description.
 2. Files can be uploaded and used as a knowledge base by Copilot. In a subsequent exercise, you'll work with file uploads.
 3. Select **X** to close the manage sources window.

Task: Explore the help feature

At the bottom right corner of the window is the help icon where you can easily access documentation and find solutions to common problems. From the help icon, you also submit a support case to the Microsoft support team if you have the appropriate role permissions.

1. Select the **Help (?)** icon.
 1. Select **Documentation**. This selection opens a new browser tab to the Microsoft Copilot for Security documentation. Return to the Microsoft Copilot for Security browser tab.
 2. Select **Help**.
 1. Anyone with access to Copilot for Security can access the self help widget by selecting the help icon then selecting the Help tab. Here you can find solutions to common problems by entering something about the problem.
 2. Users with a minimum role of Service Support Administrator or Helpdesk Administrator role can submit a support case to the Microsoft support team. If you have this role, a headset icon is displayed. Close the contact support page.

Review

In this exercise, you explored Microsoft Copilot for Security standalone experience. You explored the key landmarks of Copilot landing page including the owner settings, your past sessions, prompts and promptbooks, and the help option.

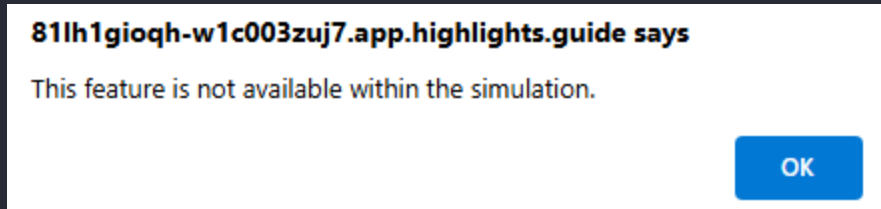
Configure the Microsoft Sentinel plugin

- 15 minutes

In this exercise, you configure the Microsoft Sentinel plugin and run some test prompts to confirm that Copilot is using the plugin.

Note

The environment for this exercise is a simulation generated from the product. As a limited simulation, links on a page may not be enabled and text-based inputs that fall outside of the specified script may not be supported. A pop-up message will display stating, "This feature is not available within the simulation." When this occurs, select OK and continue the exercise steps.



Exercise

For this exercise, you're logged in as Avery Howard and have the Copilot owner role. You'll work in both the Azure portal and the standalone experience of Microsoft Copilot for Security.

This exercise should take approximately **15** minutes to complete.

Note

When a lab instruction calls for opening a link to the simulated environment, it is generally recommended that you open the link in a new browser window so that you can simultaneously view the instructions and the exercise environment. To do so, select the right mouse key and select the option.

Task: Test a Microsoft Sentinel prompt

When working with technology, it's not uncommon to try use a feature and then realize, after some trouble-shooting, that you forgot to enable that feature. In this first task, you test a Microsoft Sentinel prompt with the Microsoft Sentinel plugin disabled. You go through this task so that you can get exposure to the information provided in the process log that helps you troubleshoot the issue.

1. Open the simulated environment by selecting this link: [Microsoft Copilot for Security](#).
2. From the prompt bar, enter the prompt **Summarize the Microsoft Sentinel incident 30342**. You can copy and paste the prompt into prompt bar. Then select the run icon.
3. The Copilot process log shows that it can't complete your request. Expand the items in the process log for more detailed information.

Task: Configure and enable the Microsoft Sentinel plugin

In this task, you'll configure the Sentinel plugin. To do this, you need to access the Azure portal to obtain the necessary information.

1. From prompt bar, select the **sources icon**



2. From the manage sources page, expand the view for the Microsoft plugins by selecting **Show 11 more** and scroll down until Microsoft Sentinel is visible.
3. Select the **Set up** button and note the parameters that need to be configured. Select the information icon next to any of the parameters. Keep this browser tab open, you'll come back to this page for each parameter to be configured.
4. Use your right mouse key to open the link to the Azure portal in a new tab or window: [Azure portal](#). It's important that access to the Azure portal and access to Copilot for Security be available as separate browser tabs, as you'll be accessing both tabs for this task.
 1. Select **Log Analytics workspaces**, it should be displayed as an icon under Azure services.
 2. Select the workspace associated with your Sentinel deployment. For this exercise, select **Woodgrove-LogAnalyticsWorkspace**.
 3. You should be on the overview page, if not select it now. From here you copy the information required to configure the Sentinel plugin.
 4. Recall that the first parameter listed on the Microsoft Sentinel settings page is the Default workspace name. **Hover over the workspace name**, until the clipboard icon is displayed. Select **Copy to clipboard**.
 5. Keep this browser tab open as you'll be referring to the information on this page for each parameter to be configured.
5. Switch back to the Copilot browser tab. Place your mouse cursor in the workspace name field and right-click to paste the contents of the clipboard to the clipboard. The workspace name is added to the field.
6. Repeat the steps until you have configured the remaining two fields. Once the all the fields are populated, select **Save**.
7. Make sure toggle switch for the Sentinel plugin is enabled, then close the manage sources window by selecting the **X**.

Task: Retest the Microsoft Sentinel prompt

Now that the Sentinel plugin is enabled, you'll run the prompt you tried earlier. With the prompt successfully executed, you'll save the prompt to the pin board and get a link to the session so you can share it with a colleague.

1. Once you've configured the plugin, you need to create a new session to rerun the Sentinel prompt. From the top of the page, select **Microsoft Copilot for Security**.
2. In the prompt bar, enter the prompt **Summarize the Microsoft Sentinel incident 30342**. You can copy and paste the prompt into the prompt bar. Then select the run icon.
3. The Copilot process log shows that the prompt executed successfully by displaying green check marks.
4. Select the **box icon**



next to the pin icon to select the response. Selecting the the **Pin icon**



pins the response to the pin board, which automatically opens. The pin board shows a summary for the pinned responses.

Review

In this exercise, you ran a prompt that requires the Microsoft Sentinel plugin to be enabled. The first time you ran the prompt, Copilot wasn't able to complete the request. The process log provided the information to help you troubleshoot the issue. You then configured and enabled the plugin. With the plugin enabled you were able successfully run the prompt.

Enable a custom plugin

Completed100 XP

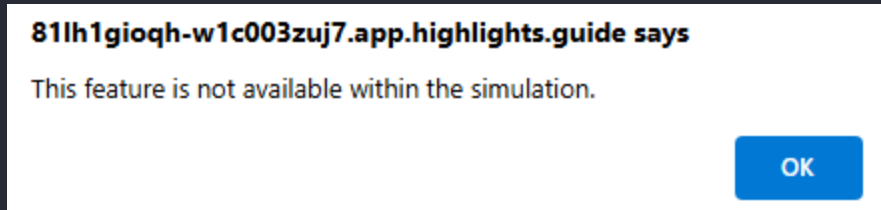
- 10 minutes

In this exercise, you experiment with a custom plugin. You start by checking the owner settings for who can add and manage their own custom plugins and who can add and manage custom plugins for everyone in the organization. Once you have configured the owner settings, you upload the file for your custom plugin. Uploading the files adds the plugin capability to Copilot. Once the plugin is added, you validate that it shows up as a system capability and start using it.

The creation of the YAML or JSON plugin manifest file, which describes metadata about the plugin and how to invoke it, is outside the scope of this content, but you can obtain more information by visiting [Create your own custom plugins](#).

Note

The environment for this exercise is a simulation generated from the product. As a limited simulation, links on a page may not be enabled and text-based inputs that fall outside of the specified script may not be supported. A pop-up message will display stating, "This feature is not available within the simulation." When this occurs, select OK and continue the exercise steps.



Exercise

For this exercise, you're logged in as Avery Howard and have the Copilot owner role. You'll work in Microsoft Copilot for Security and will be accessing a GitHub repository to download the sample manifest file for the plugin.

This exercise should take approximately **10** minutes to complete.

Note

When a lab instruction calls for opening a link to the simulated environment, it is generally recommended that you open the link in a new browser window so that you can simultaneously view the instructions and the exercise environment. To do so, select the right mouse key and select the option.

Before you start

For this exercise, you'll be using a sample .yaml file, 'KQL_DefenderExample.yaml.'

1. Select the link [KQL_DefenderExample.yaml](#) to access the sample file.
2. Select the **Download raw file**



icon. Save the file on your local computer, as you will need it later.

Alternatively, because this is a simulation, you can create the file named 'KQL_DefenderExample.yaml.' Because this is a simulation, the contents of the file you create won't matter. The system capabilities and prompt responses shown in the simulation, however, are based on the actual file.


Task: Update owner settings for custom plugins

In this task, you configure Copilot so that Copilot owners and contributors can add and manage their own custom plugins and for everyone in the organization.

1. Open the simulated environment by selecting this link: [Microsoft Copilot for Security](#).
2. Select the **Home menu** (hamburger) icon
3. Select **Owner settings**.
4. Under Plugins for Copilot for Security,
 1. Set "Who can add and manage their own custom plugins" to **Contributors and owners**.
 2. Set "Who can add and manage custom plugins for everyone in the organization" to **Contributors and owners**.
5. Return to the landing page. Select **Microsoft Copilot for Security** next to the home menu (hamburger) icon.

Task: Upload the file for your custom plugin

In this task, you upload the file named, KQL_DefenderExample.yaml, that you downloaded in the 'Before you start' section of this exercise.

1. From the prompt bar on the Copilot landing page, select the **sources** icon.
2. On the Manage sources window, scroll down until you get to the Custom plugins. Select the **Add plugin**
 button. This opens the Add a plugin window.
3. In the Add a plugin window, ensure the setting for Who can use this plugin is set to **Just me**.
4. For this exercise, select **Copilot for Security Plugin** as this is the format for the .yaml file of your custom plugin.
5. From the upload box that appears, select **Upload file**, then select the file you previously downloaded to your local computer, **KQL_DefenderExample.yaml** then select **Add**.
6. On the custom plugins page, the plugin has been added and is enabled. Note the private tag.

7. Select the **Settings** icon. The settings icon shows basic plugin information. Note the name and brief description. This is a basic sample plugin so there are no configuration parameters to configure. If there were API keys or sign-in credentials required for the plugin, this is where they would be configured, like the exercise where you configured the Microsoft Sentinel plugin. Here you can also delete the plugin. Select Cancel to exit the page.
8. Close the manage sources window by selecting the **X** on the top right of the window.

Task: Test the custom plugin

In this task, you verify the capability enabled by the plugin can be accessed from the prompts icon and you test it.

1. From the prompt bar, select the **Prompts** icon.
2. Select **See all system capabilities**.
3. Scroll all the way down until you get to **My sample Defender KQL** plugin. Listed below the plugin name is the capability (prompt) enabled by the plugin. Select **Get Latest Emails by Recipient** to run the prompt. For future reference you can search by this capability (prompt) name.
4. Enter email address of a user whose email you need to audit: [nosv32@woodgrove.ms](#).
5. As with any prompt, you can select the response and pin it to the pin board, you can share it, edit it, and more.

Review

In this exercise, you enabled a custom plugin by uploading the .yaml file for the plugin and then tested the capability supported by the plugin.

Explore file uploads as a knowledge base

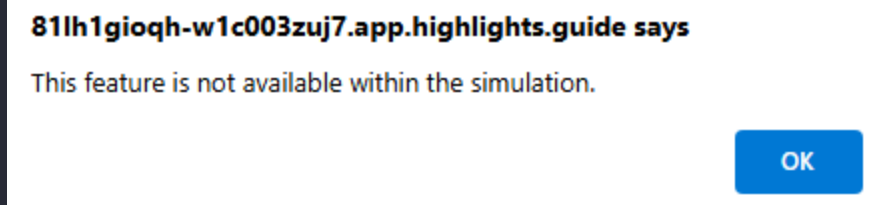
Completed 100 XP

- 10 minutes

In this exercise, you go through the process of integrating a knowledge base into Copilot, using file upload and then you do some basic testing with prompts that pull information from that knowledge base.

Note

The environment for this exercise is a simulation generated from the product. As a limited simulation, links on a page may not be enabled and text-based inputs that fall outside of the specified script may not be supported. A pop-up message will display stating, "This feature is not available within the simulation." When this occurs, select OK and continue the exercise steps.



Exercise

For this exercise, you're logged in as Avery Howard and have the Copilot owner role. For all the tasks in this exercise, you'll work in the Copilot standalone experience.

This exercise should take approximately **10** minutes to complete.

Note

When a lab instruction calls for opening a link to the simulated environment, it is generally recommended that you open the link in a new browser window so that you can simultaneously view the instructions and the exercise environment. To do so, select the right mouse key and select the option.

Before you start

For this exercise, you'll be using a sample file, 'Woodgrove Corporate Data Handling Policy.pdf.'

1. Select the link [Woodgrove Corporate Data Handling Policy.pdf](#) to access the sample file.
2. Select the **Download raw file**




icon. Save the file on your local computer, as you'll need it later.

Alternatively, because this is a simulation, you can create the file named 'Woodgrove Corporate Data Handling Policy.pdf.'
Because this is a simulation, the contents of the file you create won't matter. The prompt responses shown in the simulation,

however, are based on the actual file.

Task: Configure Copilot to support file uploads

In this task, you start by attempting a file upload but realize that there's no way to actually upload a file. This is an indication that the file upload option isn't configured. As a user with the Copilot owner role, you enable file uploads and then test using a file as a knowledge base for Copilot.

1. Open the simulated environment by selecting this link: [Microsoft Copilot for Security](#).
2. To access file uploads, select the **sources icon**

from the prompt bar.
3. From the manage sources page, select **Files**.
4. If there's no option to actually upload a file, it's because the owner setting that controls this option has been changed from the default. After conferring with the other Copilot owner, you realize this was disabled in error and agree this should be set.
 1. Close the manage source window by selecting the **X** on the top right corner of the window.
 2. Select the **Home** menu icon (hamburger icon).
 3. Select **Owner settings**.
 4. Scroll-down to **Files**. Select the drop-down and set it to **Contributors and owners can upload files**.
5. Return to the landing page. Select **Microsoft Copilot for Security** next to the home menu (hamburger) icon.

Task: Upload a file and run test prompts

In this task, you upload a file and proceed to run prompts that use that file.

1. From the landing page, select the **Sources** icon located in the promptbar.
2. From the Manage sources page, select **Files**.
3. Select **Upload file**. Upload the file **Woodgrove Corporate Data Handling Policy.pdf** that you previously downloaded or created. Once the file is uploaded, close the manage sources window.
4. With the files uploaded, you can now try some prompts. In the prompt bar, you need to mention "uploaded files" if you want Copilot to reason over your available files. You can also include the file name if you would like to guide Copilot to reason over a specific file. Enter the following prompts. You can use copy/paste:

1. Prompt: **Summarize the uploaded file Woodgrove Corporate Data Handling Policy.pdf**. The process log shows that Copilot chose file uploads and successfully processed the prompt.
2. Prompt: **Based on the uploaded file Woodgrove Corporate Data Handling Policy.pdf what data handling policies should I consider implementing in Microsoft Purview**. The process log shows that Copilot chose Microsoft Purview. The prompt response demonstrates the power of Copilot. Copilot maintains the context of the previous prompt response and integrates that information with the capability of Microsoft Purview. Although not shown in this exercise, Copilot can reason across multiple files.

Review

In this task, you configured to allow contributors and owners to upload files, you uploaded a file, and tested prompts that reasoned over the uploaded file.

Create a custom promptbook

Completed100 XP

- 10 minutes

In this exercise, you create a custom promptbook from an existing session and then run that promptbook.

Note

The environment for this exercise is a simulation generated from the product. As a limited simulation, links on a page may not be enabled and text-based inputs that fall outside of the specified script may not be supported. A pop-up message will display stating, "This feature is not available within the simulation." When this occurs, select OK and continue the exercise steps.

81lh1gioqh-w1c003zuj7.app.highlights.guide says

This feature is not available within the simulation.

OK

Exercise

For this exercise, you're logged in as Avery Howard and have the Copilot owner role. You'll work in the standalone experience of Microsoft Copilot for Security.

This exercise should take approximately **10** minutes to complete.

Note

When a lab instruction calls for opening a link to the simulated environment, it is generally recommended that you open the link in a new browser window so that you can simultaneously view the instructions and the exercise environment. To do so, select the right mouse key and select the option.

Task: Create the promptbook from an existing session

In this task, you create the promptbook. As part of the process, you templatize one of the prompts by editing the prompt with an input parameter, and then add a new prompt.

1. Open the simulated environment by selecting this link: [Microsoft Copilot for Security](#).
2. There's a session from earlier in the day that identified failed logins that you want to use. Since that session isn't listed on the landing page, select **View all sessions**.
3. Select the session labeled, **what are the last three failed logins**, it's the last session on the My Sessions list.
4. The complete session is displayed. Scroll up/down to verify two prompts are listed.
5. To include a subset of all the prompts, you can select the box next to each individual prompt. Or you can select the box next to the pin icon to include all the prompts. In this case, you want to select all the prompts from the session. Select the **box icon**







next to the pin icon to select all the prompts.

6. Now that you've selected the prompts, select the **Create promptbook**



icon. The Create a promptbook window opens. Here you populate the name, tags, and description fields for the promptbook, you configure an input parameter, and add a prompt. For the simulation, we've provided the input values to use. You can use copy/paste to enter those values or type them in as shown.

1. Name: **Failed logins**
2. Tags: **Microsoft Entra**

3. Description: **Find the last failed logins**
4. The first prompt is to show the last three failed logins. For your custom promptbook, you want to replace the number three with an input parameter. To configure the input parameter, place your mouse over the first prompt, then select the **edit**  icon.
 1. Replace the word three with an easily understood parameter that contains no spaces and is delineated with angle brackets. For this simulation, enter `<number>`.
 2. To confirm the edit, select the checkmark  icon. The number parameter is now listed in the section labeled "Inputs you'll need." For this promptbook, this is the only input needed, but you can create promptbooks that use multiple inputs.
5. For your promptbook, you'll add a new prompt. Select **+ Add prompt**.
 1. Select the **edit**  icon.
 2. Enter **What are the authentication methods for the failed logins.**
 3. Select the checkmark  icon.
6. The next step is to select who can use this promptbook. Select the drop-down to view the options. For now, leave the setting to **Just me**.
7. To create the custom promptbook, select **Create**.
8. With your promptbook created, you can choose to view the details, share the promptbook, or go to the promptbook library. Select **Promptbook library**.

Task: Run the promptbook

In this task, you explore the options available for the newly created promptbook and run the promptbook.

1. Select **My promptbooks**.
2. Place your mouse over the newly created promptbook, until it's highlighted. With the promptbook highlighted select the **ellipses** to view the available options. Select the ellipses again to close the window with the available options.

3. Select the **run**



icon to start a new session.

1. You want Copilot to return information on the last **two** failed logins.
2. Select the **Run** button.
4. Review the responses generated by Copilot.

Review

In this exercise, you created a custom promptbook from an existing session and ran that promptbook.

Explore the capabilities of Copilot in Microsoft Defender XDR

100 XP

- 30 minutes

In this exercise, you investigate an incident in Microsoft Defender XDR. As part of the investigation, you explore the key features of Microsoft Copilot in Microsoft Defender XDR, including incident summary, device summary, script analysis, and more. You also pivot your investigation to the standalone experience and use the pin board as a way to share details of your investigation with your colleagues.

Note

The environment for this exercise is a simulation generated from the product. As a limited simulation, links on a page may not be enabled and text-based inputs that fall outside of the specified script may not be supported. A pop-up message will display stating, "This feature is not available within the simulation." When this occurs, select OK and continue the exercise steps.

81lh1gioqh-w1c003zuj7.app.highlights.guide says

This feature is not available within the simulation.

OK

Exercise

For this exercise, you're logged in as Avery Howard and have the Copilot owner role. You'll work in Microsoft Defender, using the new unified security operations platform, to access the embedded Copilot capabilities in Microsoft Defender XDR. Towards the end of the exercise, you pivot to the standalone experience of Microsoft Copilot for Security.

This exercise should take approximately **30** minutes to complete.

Note

When a lab instruction calls for opening a link to the simulated environment, it is generally recommended that you open the link in a new browser window so that you can simultaneously view the instructions and the exercise environment. To do so, select the right mouse key and select the option.

Task: Explore Incident summary and guided responses

1. Open the simulated environment by selecting this link: [Microsoft Defender portal](#).
2. From the Microsoft Defender portal:
 1. Expand **Investigation & response**.
 2. Expand **Incidents & alerts**.
 3. Select **Incidents**.
3. Select the first incident in the list, **Incident Id: 30342** named Human-operated ransomware attack was launched from a compromised asset (attack disruption).
4. This is a complex incident. Defender XDR provides a great deal of information, but with 72 alerts it can be a challenge to know where to focus. On the right side of the incident page, Copilot automatically generates an **Incident summary** that helps guide your focus and response. Select **See more**.

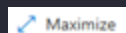
1. Copilot's summary describes how this incident has evolved, including initial access, lateral movement, collection, credential access and exfiltration. It identifies specific devices, indicates that the PsExec tool was used to launch executable files, and more.
2. These are all items you can leverage for further investigation. You explore some of these in subsequent tasks.
5. Scroll down on the Copilot panel and just beneath the summary are **Guided responses**. Guided responses recommend actions in support of triage, containment, investigation, and remediation.
 1. The first item in the triage category is to Classify this incident. Select **Classify** to view the options. Review the guided responses in the other categories.
 2. Select the **Status** button at the top of the guided responses section and filter on **Completed**. Two completed activities show labeled as Attack Disruption. Automatic attack disruption is designed to contain attacks in progress, limit the impact on an organization's assets, and provide more time for security teams to remediate the attack fully.
6. Keep the incident page open, you'll use it in the next task.

Task: Explore device and identity summary

1. From the incident page, select the first alert **Suspicious URL clicked**.
2. Copilot automatically generates an **Alert summary**, which provides a wealth of information for further analysis. For example, the summary identifies suspicious activity, it identifies data collection activities, credential access, malware, discovery activities, and more.
3. There's a lot of information on the page, so to get a better view of this alert, select **Open alert page**. It's on the third panel on the alert page, next to the incident graph and below the alert title.
4. On the top of the page, is card for the device parkcity-win10v. Select the ellipses and note the options. Select **Summarize**. Copilot generates a **Device summary**. It's worth noting that there are many ways you can access device summary and this is just one convenient method. The summary shows the device is a VM, identifies the owner of the device, it shows its compliance status against Intune policies, and more.
5. Next to the device card is a card for the owner of the device. Select **parkcityjonaw**. The third panel on the page updates from showing details of the alert to providing information about the user Jonathan Wolcott, an account executive, whose Microsoft Entra ID risk and Insider risk severity are classified as high. These aren't surprising given what you've learned from the Copilot incident and alert summaries. Select the ellipses then select **Summarize** to obtain an identity summary generated by Copilot.
6. Keep the alert page open, you'll use it in the next task.

Task: Explore script analysis

1. Let's Focus on the alert story. Select **Maximize**



, located on the main panel of the alert, just beneath the card labeled 'partycity\jonaw' to get a better view of the process tree. From maximized view, you begin to get a clearer view of how this incident came to be. Many line items indicate that powershell.exe executed a script. Since the user Jonathan Wolcott is an account executive, it's reasonable to assume that executing PowerShell scripts isn't something this user is likely to be doing regularly.

2. Expand the first instance of **powershell.exe execute a script**, it's the one showing the timestamp of 4:57:11 AM. Copilot has the capability to analyze scripts. Select **Analyze**.
 1. Copilot generates an analysis of the script and suggests it could be a phishing attempt or used to deliver a web-based exploit.
 2. Select **Show code**. The code shows a defanged URL.
3. There are several other items that indicate powershell.exe executed a script. Expand the one labeled **powershell.exe - EncodedCommand...** with the timestamp 5:00:47 AM. The original script was base 64 encoded, but Defender has decoded that for you. For the decoded version, select **Analyze**. The analysis highlights the sophistication of the script used in this attack.
4. Close the alert story page by selecting the **X** (the X that is to the left of Copilot panel). Now use the breadcrumb to return to the incident. Select **Human-operated ransomware attack was launched from a compromised asset (attack disruption)**.

Task: Explore file analysis




1. You're back at the incident page. In the alert summary, Copilot identified the file Rubeus.exe, which is associated with the 'Kekeo' malware. You can use the file analysis capability in Defender XDR to see what other insights you can get. There are several ways to access files. From the top of the page, select the **Evidence and Response** tab.
2. From the left side of the screen select **Files**.
3. Select the first item from the list with the entity named **Rubeus.exe**.
4. From the window that opens, select **Analyze**. Copilot generates a summary.
5. Review the detailed file analysis that Copilot generates.
6. Close the file analysis window.

Task: Pivot to the standalone experience

This task is complex and requires the involvement of more senior analysts. In this task, you pivot your investigation and run the Defender incident promptbook so the other analysts have a running start on the investigation. You pin responses to the pin board and generate a link to this investigation that you can share with more advanced members of the team to help investigate.

1. Return to the incident page by selecting the **Attack story** tab from the top of the page.
2. Select the ellipses next to Copilot's Incident summary and select **Open in Copilot for Security**.
3. Copilot opens in the standalone experience and shows the incident summary. You can also run more prompts. In this case, you'll run the promptbook for an incident. Select the **prompt icon**



1. Select **See all promptbooks**.
2. Select **Microsoft 365 Defender incident investigation**.
3. The promptbook page opens and asks for the Defender Incident ID. Enter **30342** then select **Run**.
4. Review the information provided. By pivoting to the standalone experience and running the promptbook, the investigation is able to invoke capabilities from a broader set security solution, beyond just Defender XDR, based on the plugins enabled.
4. Select the **box icon**

next to the pin icon to select all the prompts and the corresponding responses, then select the **Pin icon**

to save those responses to the pin board.
5. The pin board opens automatically. The pin board holds your saved prompts and responses, along with a summary of each one. You can open and close the pin board by selecting the **pin board icon**

6. From the top of the page, select **Share** to view your options. By sharing the incident via a link or email, people in your organization with Copilot access can view this session. Close the window by selecting the **X**.
7. You can now close the browser tab to exit the simulation.

Review

This incident is complex. There's a great deal of information to digest and Copilot helps summarize the incident, individual alerts, scripts, devices, identities, and files. Complex investigations like this may require the involvement of several analysts. Copilot facilitates this by easily sharing details of an investigation.

Explore the capabilities of Copilot in Microsoft Purview

Completed100 XP

- 30 minutes

Microsoft Copilot for Security is accessible within Microsoft Purview data security and compliance solutions, including Data Loss Prevention (DLP), Insider Risk Management, Communication Compliance, and eDiscovery (Premium).

In this exercise, you explore the Copilot summarization capabilities available in each of these solutions. You start by verifying that the Microsoft Purview plugin is enabled.

Note

The environment for this exercise is a simulation generated from the product. As a limited simulation, links on a page may not be enabled and text-based inputs that fall outside of the specified script may not be supported. A pop-up message will display stating, "This feature is not available within the simulation." When this occurs, select OK and continue the exercise steps.

81lh1gioqh-w1c003zuj7.app.highlights.guide says

This feature is not available within the simulation.

OK

Exercise

For this exercise, you're logged in as Avery Howard. You have the Copilot owner role and you have specific role permissions required for access to each of the afore mentioned Microsoft Purview solutions.

You'll work with specific Microsoft Purview solutions, using the new Microsoft Purview portal, and access the embedded Copilot capabilities of those solutions.

This exercise should take approximately **30** minutes to complete.

Note

When a lab instruction calls for opening a link to the simulated environment, it is generally recommended that you open the link in a new browser window so that you can simultaneously view the instructions and the exercise environment. To do so, select the right mouse key and select the option.

Task: Enable the Microsoft Purview plugin

In this task, you enable the Microsoft Purview plugin. For this task, you work in the standalone experience.

1. Open the simulated environment by selecting this link: [Microsoft Copilot for Security](#).
2. From the Microsoft Copilot for Security landing page, select the **Sources icon**



in the prompt bar.

1. From the manage sources window, under the Microsoft plugins, select **Show 11 more**.
2. Scroll down so that the Microsoft Purview plugin is visible.
3. Select the **Information icon**



. Note the instructions then close the plugins page by selecting the **X** on the top-right corner of the manage sources window.

3. Select the **Home menu**



, often referred to as the hamburger icon.

1. Select **Owner settings**.
 2. Enable the toggle switch next to **Allow Copilot for Security to access data from your Microsoft 365 services**.
 3. Return to the Copilot home page, by selecting **Microsoft Copilot for Security** on the top-left of the page next to the home menu (hamburger) icon.
4. Now that you've enabled Copilot to access data from your Microsoft 365 services, return to the plugins page and enable the Microsoft Purview plugin.
 1. From the promptbar, select the **Sources icon**.
 2. From the manage sources window, under the Microsoft plugins, select **Show 11 more**.

3. Enable the toggle switch next to Microsoft Purview to enable the plugin.
4. Close the manage sources window by selecting the **X**.

Task: Gain comprehensive summary of Insider Risk Management alerts

For this and all subsequent tasks, you explore the Copilot functionality embedded in Microsoft Purview.

In this task, you explore the value Copilot provides in summarizing an Insider Risk Management alert. You start by first reviewing an alert, without Copilot for Security. It can be challenging to know where to start your investigation when risky activities are detected over a long period of time. You'll then see how Copilot can address this same task with the click of a button.

Microsoft Copilot assumes the permissions of the user when it tries to access the data to answer queries. To access data associated with the Microsoft Purview Insider Risk Management solution, the Copilot user should have previously been assigned an appropriate role.

1. Open the environment by selecting this link: [Microsoft Purview Portal](#). A pop-up window appears that says, "Welcome to the new Microsoft Purview portal!"
 1. Select the box where it says **"This is a public preview. I agree to the terms of data flow disclosure, the preview section of the Product Terms, and Privacy Statements."**
 2. Select **Try now**.
 3. You can close the Explore all solutions pop-up by selecting the **X**. Alternatively, you can select Next to go through the information. If you go through all six information windows, you'll need to scroll-up to get back to the top of the page, when you're done.
2. From the Microsoft Purview portal, select **Insider Risk Management**.
3. Select **Alerts**.
4. Select the first alert on the list, alert ID: **86e52569**.
 1. This alert is associated with the policy, 'Potential data theft - Employee Departure.' Under User details, you can gain more context on why the user was identified as a high impact user by selecting **View all details**. Review the user details then select the **X** to close the User details window.
 2. The current page shows **All risk factors**. If you scroll down, there are even more details to consume.
 3. Select the **Activity explorer** tab, to quickly review a timeline of potentially risky activity and filter for specific risk activities associated with the alert. Select, the first activity on the list, labeled **Files accessed on SPO**. Review the information provided then select **X** to close the window.

4. Select the **User activity tab**. Here you view a scatter plot, over a one month, three months, or six months timeline; alongside details of each event.
5. With Copilot for Security, you can gain a comprehensive summary of an alert – in the single click of a button! From the top of the alert page, select **Summarize**.
 1. This comprehensive summary provides key details, including alert severity, user details like their HR offboarding event and much more!
 2. These summaries help accelerate investigations by helping you quickly gain context into user intent and timing of risky activities, enabling you to tailor your investigation with specific dates in mind and quickly pinpoint sensitive files at risk.
6. From the left navigation panel, select **Home** to return the Microsoft Purview portal. You'll return to this page in the next task.

Task: Gain comprehensive summary of Data Loss Prevention alerts.

In this task, you explore the value Copilot provides in summarizing a Data loss prevention alert. As in the previous task, you start by first reviewing an alert, without Copilot for Security. You then discover how Copilot can address this same task with the click of a button.

Microsoft Copilot assumes the permissions of the user when it tries to access the data to answer queries. To access data associated with the Microsoft Purview Data Loss Prevention solution, users should have previously been assigned an appropriate role.

1. Select **Data loss prevention**, then select **Alerts**
2. Investigating DLP alerts can be overwhelming due to the large number of sources to analyze, including apps, cloud services, email, endpoints and chat, and the varying rules and conditions of a policy.
3. Select the first alert from the list, labeled, **DLP policy match for document cardholder transaction Log.xlsx in OneDrive**.
 1. A side panel opens listing some details of this alert, including the alert status, severity, the DLP policy match, location, and user involved. From the bottom of the page, select **View details**. This opens a new browser tab.
 2. Select the **Events** tab. For the selected event, you can view event details, impacted entities and more.
 3. Select the **Classifiers** tab. Under classifiers, you can view the specific sensitive information types or trainable classifiers that were matched.
 4. You can also select File Activity. There's much information to analyze.
 5. Close this browser tab, but be sure to keep the 'Alerts|Microsoft Purview' tab open.
4. Now view the information that Copilot can generate with the click of a button.

1. From the Alerts|Microsoft Purview tab, which is showing the side panel with information about the alert, select **Summarize with Copilot**.
2. This comprehensive summary provides key details, including policy rules, source, files involved and more. Additionally, the summary pulls the user risk levels from Insider Risk Management, providing integrated insights across data security solutions. These summaries provide you with a better starting point for further investigation.
5. From the left navigation panel, select **Home** to return the Microsoft Purview portal. You'll return to this page in the next task.

Task: Gain contextual summary of Communication Compliance policy matches

In this task, you explore the capability of Copilot in Microsoft Purview Communication Compliance. Reviewing communication violations can be time-consuming, especially when reviewing lengthy content like meeting transcripts, email attachments, Teams attachments, or extensive text. Copilot can address this, and more, with the click of a button.

Microsoft Copilot assumes the permissions of the user when it tries to access the data to answer queries. To access data associated with the Microsoft Purview Communication Compliance solution, users should have previously been assigned an appropriate role.

1. From the New Microsoft Purview portal, select **View all solutions**, then select **Communication Compliance**, listed under Risk & Compliance.
2. Select **Policies**.
3. Select **Regulatory compliance** policy to identify potential regulatory compliance violations.
4. From the list of violations triggered by the policy, select the Teams communication with the subject **Happy new year valued customers!** to expand the list. Select the first item from the expanded view.
5. Communication Compliance is able to pinpoint the timestamps when a potential violation has occurred and highlight conditions matched, but there's still a good bit of text to read through.
 1. With Copilot for Security, you can gain a comprehensive summary of an alert in the single click of a button! Select **Summarize**.
 2. You can also ask follow-up questions. Use copy/paste to enter **Does this violation indicate unauthorized disclosure?**
6. From the left navigation panel, select **Home** to return the Microsoft Purview portal. You'll return to this page in the next task.

Task: Gain contextual summary of evidence collected in eDiscovery review sets (Preview)

In this task, you explore the capability of Copilot to Microsoft Purview to gain a contextual summary of evidence collected in an eDiscovery review set.

Legal investigations can take hours, days, even weeks to sift through the list of evidence collected in review sets, requiring costly resources like outside counsel to manually go through each document to determine the relevancy to the case. Copilot can significantly reduce that burden by generating summaries of conversations in a variety of languages and the documents that may be included as attachments.

Microsoft Copilot assumes the permissions of the user when it tries to access the data to answer queries. To access data associated with the Microsoft Purview eDiscovery solution, users should have previously been assigned an appropriate role.

1. From the New Microsoft Purview portal, select **View all solutions**, then select **eDiscovery**, listed under Risk & Compliance.
2. For this simulation, you're taken directly to the page for cases. From the cases page, select **Contoso stock manipulation**, then select the tab **Review sets**.
3. From the review sets page, open the review set listed **RS - Stock manipulation Teams conversation + cloud attachments**
 1. From the bottom of the Overview page, select **Open review set**.
 2. Using the filter, filter for Teams conversations:
 1. Filter - **File class**.
 2. Select an operator - **Equals any of**.
 3. Select Any - **Conversation**.
 3. From the results, select the first item on the list **#1**.
 1. Information about the conversation appears in the window to the right. **Scroll** to view the source history. There's quite a bit of text included in this teams conversation. It can be time-consuming to sift through the information.
 2. With Copilot for Security, you can gain a comprehensive summary of the conversation in the review set – in the single click of a button! Select **Summarize**. Copilot also provides prompt suggestions and the prompt bar for you to enter your own prompts in furtherance of the investigation. This helps you save time and conduct investigations more efficiently!
4. Refer back to the list of Teams conversations. This time, select the second item on the list select item **#2**.
 1. The subject is displayed in a non-English language. This is common challenge with multi-national corporation whose employees speak various languages. The window with the source conversations shows a conversation history with non-English language. Select **Summarize** to view a summary in English, which is my default language for Copilot.
 2. Within Microsoft Teams, you can send cloud attachments, which are links to documents. Expand item **#2** by selecting the **>**. The first subitem is a Word document. Select the document then select **Summarize** to have Copilot generate a

5. From the left navigation panel, select **Home** to return the Microsoft Purview portal. You'll return to this page in the next task.

Task: Create Keyword Query Language (KeyQL) queries using natural language to search in eDiscovery (Premium)

In this task, you explore the capability of Copilot in Microsoft Purview eDiscovery (Premium) to create Keyword Query Language (KeyQL) queries using natural language. Users provide a prompt in natural language and Copilot generates a query in KeyQL language, making your search iterations faster and more accurate. This feature also enables analysts, at all levels, to conduct advanced investigations using KeyQL.

Microsoft Copilot assumes the permissions of the user when it tries to access the data to answer queries. To access data associated with the Microsoft Purview eDiscovery solution, users should have previously been assigned an appropriate role.

1. From the New Microsoft Purview portal, select **View all solutions**, then select **eDiscovery**, listed under Risk & Compliance.
2. For this simulation, you're taken directly to the page for cases.
3. Select **Fabrikam vs Contoso**.
4. Select **Create a search**.
 1. Enter a search name.
 2. Enter a description.
 3. Select **Create**.
5. Add a data source
 1. Select **Add data sources**.
 2. In the search bar, enter **Sales**.
 3. From the search results, select **Sales**.
 4. From the bottom of the page, select **Save**.
6. Now use Copilot draft a query in natural language. Select **Draft a query with Copilot**.
 1. From the box labeled natural language prompt, select **View prompts**. This is a great starting point. You could look at suggested prompts to determine how to craft a natural language query for suggested prompts. For example, Find all emails containing the words budget and finance and have attachments.
 2. For this example, however, you know what you are looking for. You've been told that you need to find all conversations related to a recent acquisition. Use copy/paste to enter **Find all conversations that contain the keywords;**

acquisition, stock, Bitdefender, Frostvision, offshore.

3. When you enter your natural language prompt, you can have Copilot refine the query to ensure a more accurate query output. Select **Refine** then **Accept**.
4. Select **Generate KeyQL**. Copilot for Security refines the prompt and then in a simple click, can generate the query within seconds!
5. The purpose of this exercise is to show how easily Copilot can generate the code for a query using natural language. In your production environment, to run the generated query copy the KeyQL code into the run box and select run.

Review

With Microsoft Copilot in Microsoft Purview, data security and compliance admins can use the power of AI to assess risk exposure more quickly than is otherwise possible, directly from within Microsoft Purview solutions.

In this exercise, you explored the powerful functionality of Copilot to aid in your compliance investigations with DLP, Insider Risk Management, Communication Compliance, and eDiscovery.

Summary and resources

Completed 100 XP

- 1 minute

In this module, you went through a series of simulation-based exercises to help you effectively use Microsoft Copilot for Security in your own work environment.

You went through a first run experience using the Microsoft Copilot for Security wizard, which involved provisioning security compute units (SCU). You explored the features of the standalone experience of Copilot, including owner settings, sessions, and promptbooks. You also created your own promptbook.

The module then moved on to exercises focused on managing sources. You configured a Microsoft plugin. You added a custom plugin and ran prompts using that plugin. You integrated a knowledge base into Copilot using file upload and ran prompts that reasoned over that knowledge base.

Lastly, you explored the capabilities of Copilot embedded in Defender XDR and Purview.

Now that you completed this module, you can:

- Set Up and provision Microsoft Copilot for Security.
- Explore the standalone experience of Microsoft Copilot for Security.
- Manage sources.
- Work with prompts and promptbooks.
- Explore the features of the different embedded experiences.

Learn more

- [*Get started with Microsoft Copilot for Security*](#)
- [*Plugins overview Microsoft Copilot for Security*](#)
- [*Build your own promptbooks*](#)
- [*Microsoft Security Copilot in Microsoft Defender XDR*](#)
- [*Microsoft Copilot in Intune \(public preview\)*](#)
- [*Microsoft Copilot for Security in Microsoft Purview*](#)

Keep up the great work!



Explore use cases of Microsoft Copilot for Security

You have earned an achievement!

Congratulations, but what should you do next?