

Copilot for Security

-Attendee Lab Manual-

ANZ Roadshow



⚠ Disclaimer: All exercises in this lab are based on the current environment at Alpine Skihouse and are subject to change. Incidents, alerts, user status, and risk levels can vary over time, which may result in different responses. While we strive to keep the materials updated, we cannot guarantee their accuracy at all times.

Table of Contents

Objectives	4
Objectives	5
Exercise 1: M365 Defender.....	5
Incident Summary and Guided Response	5
Incident Report	6
Export incident data to PDF	7
File Analyzer	7
Script Analyzer.....	10
.....	10
Device Summary.....	11
Activity 2 : Copilot for Security Standalone Experience.....	12
Explore Copilot for Security Standalone Experience	12
Manage Plugins	15
Exercise 1: Effective Prompting	18
Effective vs non effective prompts	18
Building and iterating on your prompt.....	24
Sample complex prompts with output	25
Activity 4: Investigate an identity-based security incident.....	27
Investigate in standalone.....	27
Activity 5: Intune	29
Intune Policy Management	29
Intune Summarize Existing Policies and Assess Their Impact to Users and Security.....	32
Assistance to troubleshoot devices in Intune, using Copilot for Security.....	35
Activity 6 Purview: Investigate a data leakage (DLP) incident	42
Investigate in standalone.....	42
Exercise 4: Investigate BEC Fraud Attack incident.....	43
Incident Summary.....	43

Continue the incident investigation in the standalone portal.....	44
Create a promptbook from your session	46
Activity 7: Extensibility.....	49
Objectives	49
Exercise 1: Knowledge Base Integration	49
File Upload.....	49
Using the uploaded Policy document in Copilot for Security	50
Review Azure AI Search in Copilot for Security	50
Exercise 2: KQL Sentinel Cost Custom Plugin	51
Configure and review the KQL Custom Plugin	51
Using the plugin in Copilot for Security	53
Exercise 3: Using KQL and API Plugins to investigate a custom GCP Log	55
Configure and review the plugins	55
Verify ADX cluster and query access.....	56
Using the plugins in Copilot for Security.....	57
Activity 4: Automation (Optional as do not have lab permissions)	60
Objectives	60
Exercise 1: Create Threat Bulletin Logic App.....	60
Open the Logic App in Logic App Designer	61
Add Actions	61

Estimated time to complete this lab

Objectives

This document is designed to be an immersive and collaborative experience focused on harnessing the power of Copilot to enhance security measures.

Microsoft Copilot for Security (Copilot for Security) is a generative AI-powered security solution that helps increase the efficiency and capabilities of defenders to improve security outcomes at machine speed and scale.

This document is a hands-on lab session where participants will dive deep into Copilot's capabilities for threat detection, incident response, and overall security enhancement. It is an opportunity to explore real-world scenarios, create custom prompts, and fine-tune security strategies using Copilot's advanced features.

Activity 1: Embedded

Objectives

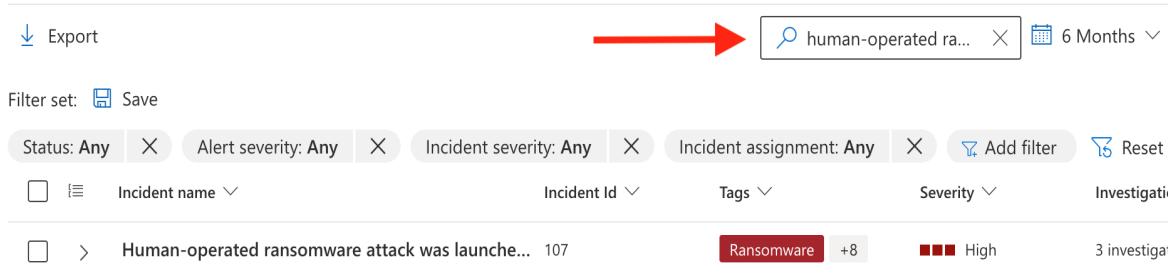
The objective of this activity is to familiarize participants with Copilot for Security embedded features and demonstrate the value they bring. Through hands-on exercises, participants will learn search for incidents, review summaries, analyze scripts and files, summarize device information, use guided responses to resolve incidents, generate KQL queries, and create incident reports. Additionally, participants will gain experience with Intune and Purview, managing policies, troubleshooting devices, and summarizing Insider Risk Management alerts.

Exercise 1: M365 Defender

This exercise involves investigating a Human Operated Ransomware attack using Microsoft Defender and Copilot for Security. You'll search for the incident, review the summary, analyze scripts and codes, analyze files, summarize device information, use guided responses to resolve incidents, generate KQL queries and create incident reports.

Incident Summary and Guided Response

1. Go to **Investigation & response > Incidents & alerts > Incidents on** in the [Microsoft Defender portal](#) (Incident: **107**, Direct URL: [Incident - Microsoft Defender](#)). If needed in the incident search bar, start typing "**Human-Operated Ransomware**" and hit enter



A screenshot of the Microsoft Defender portal's search interface. At the top right, there is a search bar containing the text "human-operated ra...". A large red arrow points from the left towards this search bar. To the right of the search bar are filter options: "6 Months" (with a calendar icon), "Reset" (with a circular arrow icon), and "Add filter" (with a plus sign icon). Below the search bar are several filter buttons: "Status: Any", "Alert severity: Any", "Incident severity: Any", "Incident assignment: Any", "Save" (with a save icon), and "Reset" (with a circular arrow icon). Further down, there are more filters: "Incident name" (with a dropdown arrow), "Incident Id" (with a dropdown arrow), "Tags" (with a dropdown arrow), "Severity" (with a dropdown arrow), and "Investigati" (partially visible). At the bottom of the search bar area, there is a list of incidents: "Human-operated ransomware attack was launche... 107" (with a checkbox and a right arrow icon), "Ransomware +8" (with a red button), "High" (with a red square icon), and "3 investiga" (partially visible).

2. Open the incident page by clicking on it >Copilot automatically creates an **Incident Summary** upon opening the page.

 **Tip:** Review the generated summary and involved files. This is a great example of ROI to business

3. The Copilot pane appears on the right side also shows the **Guided Response cards**.

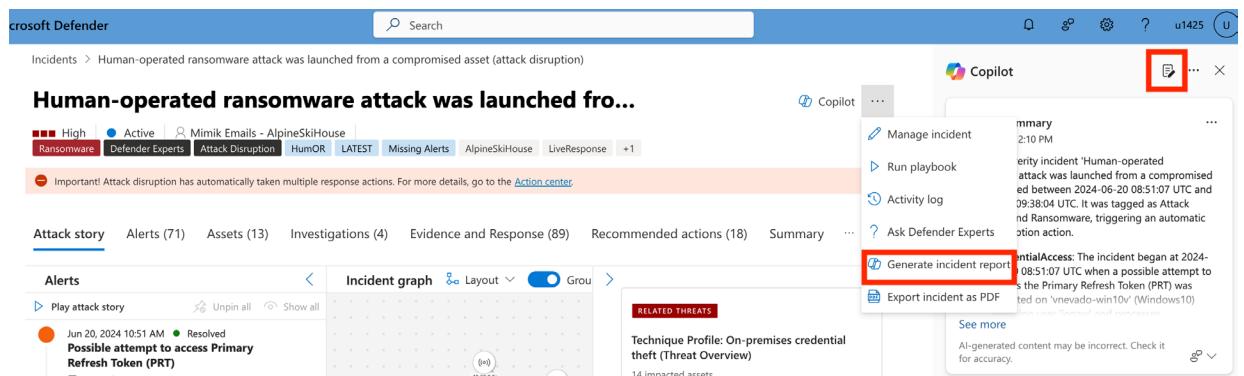
 **Tip:** Each card contains information about the recommended action or an action completed during attack disruption, including the affected assets, such as users, devices, or mailboxes, where the action is recommended. The cards also highlight when a recommended action has been completed, emphasizing the details of the attack disruption.

4. **Close the generated summary** by clicking the "X" button located at the top-right corner of the summary window.

Incident Report

5. Select the report icon found on top of the Copilot side panel to generate the Incident Report.

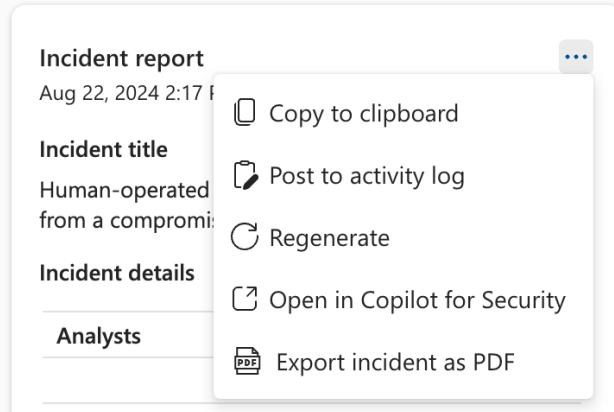
 **Tip:** Alternatively, you can select the More actions ellipsis (...) on the incident page, then select Generate incident report and review the report



6. Open the incident's activity log by clicking on the **More actions ellipsis (...)** and selecting **Activity log** on the incident pane.

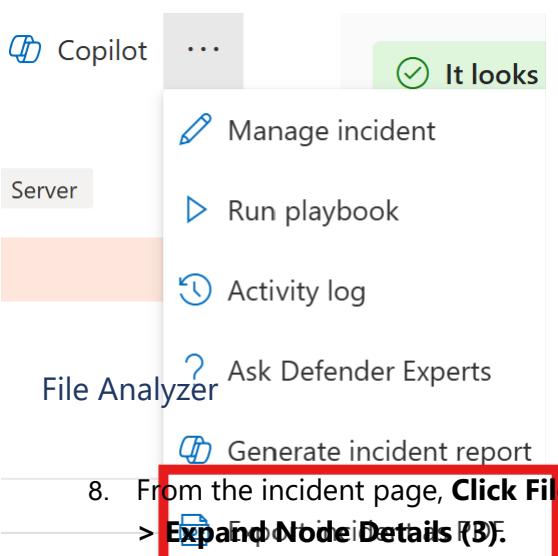
 **Tip:** Refer to the complexity of manually summarizing long activity logs into one report and the ability of Copilot to summarize this efficiently in the incident report.

- Once generated, the report can be copied to your preferred system “**Copy to clipboard**” or posted to the incident’s activity log for record-keeping. By posting the report to the activity log, SOC teams can refer to the actions of an incident for future decision-making.

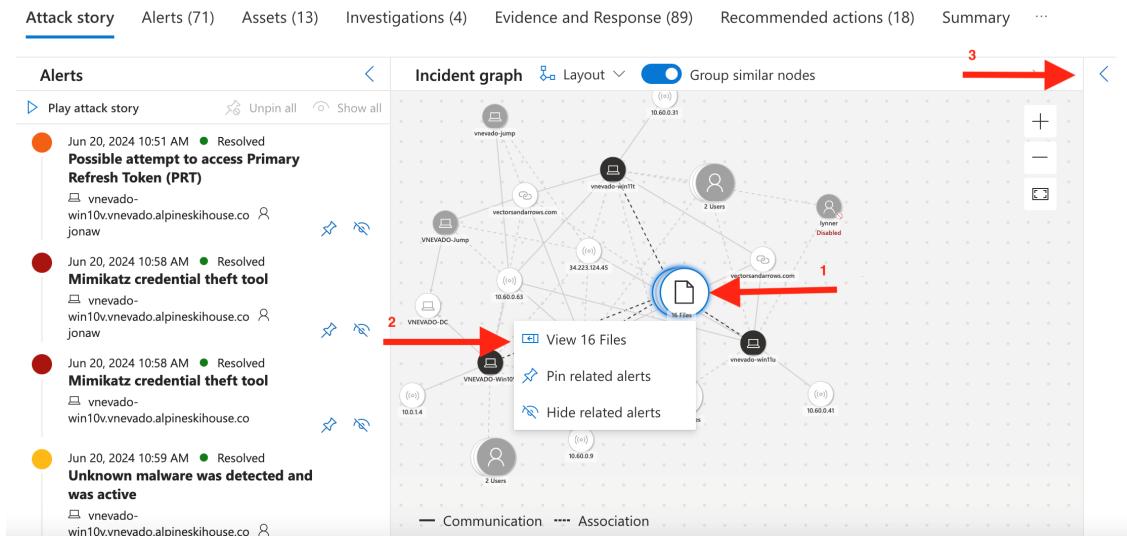


Export incident data to PDF

You can export the incident data to PDF to create a report that you can easily share with stakeholders. The exported incident data contains relevant information like the **attack story**, **impacted assets**, **relevant alerts**, and **AI-generated content from Copilot**, like the **incident summary and incident report**. With this capability, security teams can quickly export more incident information for post-incident discussions within team members or with other stakeholders.



 **Tip:** You can also choose a file to investigate on an alert page.



The screenshot shows the Copilot for Security interface. The top navigation bar includes 'Attack story', 'Alerts (71)', 'Assets (13)', 'Investigations (4)', 'Evidence and Response (89)', 'Recommended actions (18)', 'Summary', and a '...' button. The 'Alerts' section on the left lists four resolved alerts related to Mimikatz credential theft tools and unknown malware. The 'Incident graph' section on the right shows a network of nodes representing hosts and users, with connections indicating communication and associations. A specific node for 'mimikatz.exe' is highlighted with a blue box and a red arrow. A context menu for this node is open, showing options: 'View 16 Files' (highlighted with a blue box), 'Pin related alerts', and 'Hide related alerts'. A red arrow also points to the 'View 16 Files' option in the menu. The bottom of the graph pane has legends for 'Communication' and 'Association'.

9. Select the **Mimikatz.exe** or **Mimilove.exe** file to investigate.

> [Back to incident details](#)

16 Files

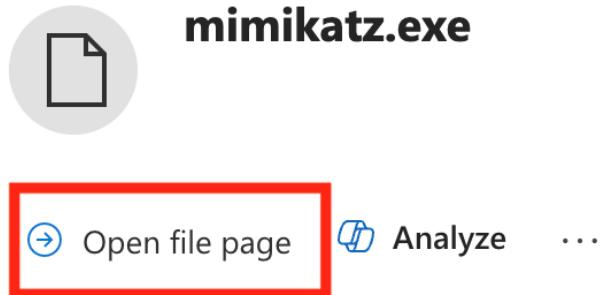
Name

[notepad.exe](#)

[mimikatz.exe](#)

[mimikatz.exe](#)

10. Then select **Open File Page**. Copilot automatically generates an analysis upon opening a file page.



Tip: The file analysis results generated by Copilot typically include Assessment of the file, detection name if malicious/unwanted, key file information, Highlights strings found, lists API calls used, and relevant certificate information.

File analysis ...

Oct 18, 2024 1:29 AM

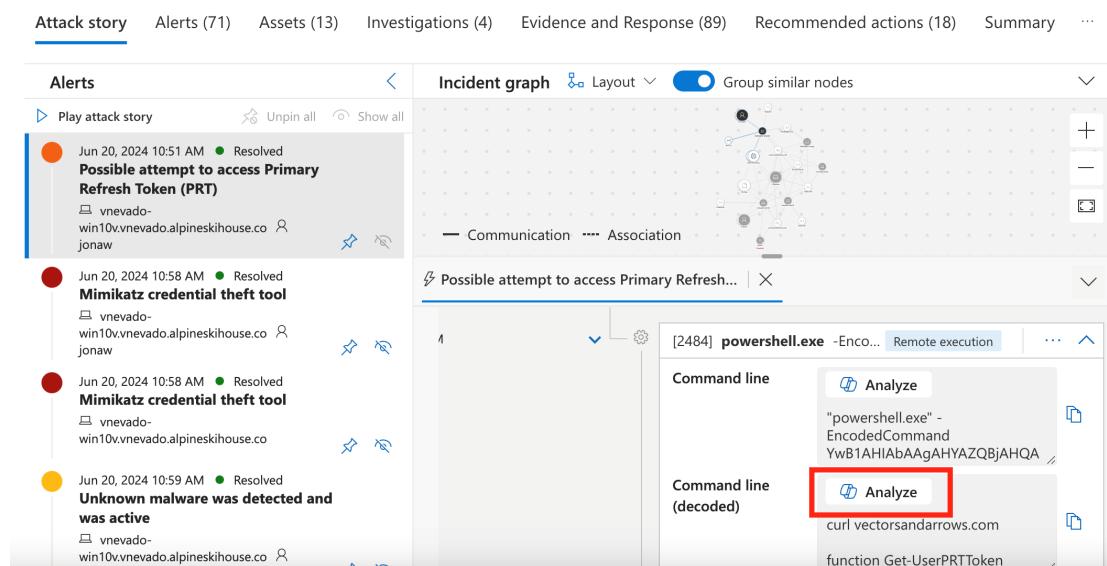
Overview

The VirusTotal scan results indicate that 63 out of 73 engines have detected the file as malicious, with Microsoft labeling it as HackTool:Win32/Mimikatz.gen!H. The absence of digital certificate information raises additional concerns about the file's authenticity and trustworthiness. The file is identified as malware, and the PE metadata shows a size of 40 KB with the company name listed as "gentilkiwi (Benjamin DELPY)," which is associated with the creator of Mimikatz, a known hacking tool. These factors collectively suggest a high risk level, warranting further scrutiny.

Script Analyzer

11. Within the incident page , select the PRT alert on the left pane, select the PowerShell script in the process tree with [2484] **powershell.exe** with the curl command line. Click **Analyze** to start the analysis.

 **Tip:** This script that uses curl via PowerShell to access the PRT is a great example to see script analyzer in action.



Script analysis

Oct 18, 2024 1:47 AM

The script performs several actions to locate and execute 'browsercore.exe' to retrieve cookies from 'hps://0pm4injih-tjfvl43pvrn.app.highlights.guide/common/oauth2/authorize', save the data to 'prtt.bin', download 'psexec.exe' and 'mimikatz_trunk.zip', extract login passwords using 'mimikatz.exe', and perform a pass-the-hash attack using the extracted NTLM hashes. The script interacts with URLs such as 'hps://live.sysinternals.com/psexec.exe' and 'h**ps://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip', and targets the domain 'alpineskihouse.co'.

1. The script attempts to locate and execute 'browsercore.exe' from specific directories to retrieve cookies from a specified URL.

Show code

2. The script constructs a JSON body to request cookies from `h**ps://0pm4injih-tjfvl43pvrn.app.highlights.guide/common/oauth2/authorize` and sends it using 'browsercore.exe'.

3. The script captures the response from `browsercore.exe` and processes it to extract data.

Show code

4. The script saves the extracted data to a file named `prtt.bin` in the temporary directory.

Show code

5. The script downloads `psexec.exe` from `'h**ps://live.sysinternals.com/psexec.exe'` and saves it as `'notepad.exe'` in the temporary directory.

Show code

6. The script downloads `mimikatz_trunk.zip` from `'h**ps://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip'` and extracts it to a specified directory.

Show code

7. The script runs `mimikatz.exe` to extract login passwords and processes the output to extract usernames, domains, and NTLM hashes.

Show code

8. The script uses the extracted NTLM hashes to perform a pass-the-hash attack using `mimikatz.exe` and `'notepad.exe'`.

Show code

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

Device Summary

12. Within the incident page ,select the **Assets tab**
13. Click **Devices** and click device **vnevado-win10r.vnevado.alpineskihouse.co** on the Right.

The screenshot shows the Microsoft Endpoint Manager interface. At the top, there are three tabs: 'Attack story', 'Alerts (71)', and 'Assets (13)', with 'Assets (13)' being the active tab and highlighted with a red box. Below the tabs, a sidebar on the left lists categories: 'All assets (13)' (selected), 'Devices (8)' (highlighted with a red box), 'Users (5)', 'Mailboxes (0)', 'Apps (0)', and 'Cloud Resources (0)'. To the right, a main pane displays a list of devices. The first device in the list is 'vnevado-win10r', which is also highlighted with a red box. Below the device name, it says 'No known risks' and 'Isolated'. A criticality indicator shows 'Very high'. At the bottom of the device card, there are buttons for 'Open device page', 'Summarize', 'Device value', and more options. The entire device card is also highlighted with a red box.

14. Click **Open Device page**. Copilot automatically generates an analysis upon opening the device page.

Tip: Note the owner, software vulnerability and risky settings of the device.

The screenshot shows the Copilot Device summary page for the device 'vnevado-win10r.vnevado.alpineskihouse.co'. The page includes the following sections:

- Device summary:** Last updated on Oct 18, 2024 at 1:56 AM.
- Device Name:** vnevado-win10r.vnevado.alpineskihouse.co
- Owner:** Pradeep Gupta (pradeepg@vnevado.alpineskihouse.co)
- Device Model:** Virtual Machine
- Exposure Level:** High
- Security Posture:** The device has several risky settings and outdated antivirus definitions, which increase its vulnerability to attacks.
- Vulnerable Software:** Multiple critical and high-severity software vulnerabilities are present on the device.
- Compliance State:** Not provided
- NonCompliance Reasons:** Not provided
- Infrequent Logon Users:** Not provided
- Infrequent Logon Users:** Not provided (repeated entry)
- Antivirus:** Cloud Connectivity - Failed communication with the cloud service, reducing protection against malware.
- Antivirus:** Signature - Last updated 1 week ago, potentially exposing the device to new viruses.
- Firewall:** Disable merging of local Microsoft Defender Firewall connection rules with group policy firewall rules for the Public profile - Off, increasing the risk of remote exploitation.
- Firewall:** Disable Microsoft Defender Firewall notifications when programs are blocked for Private profile - Off.
- Firewall:** Disable Microsoft Defender Firewall notifications when programs are blocked for Domain profile - Off.
- Firewall:** Disable Microsoft Defender Firewall notifications when programs are blocked for Public profile - Off.
- Attack Surface Reduction:** Off, reducing the effectiveness of blocking common attack techniques.
- Vulnerable software:** A list of vulnerabilities including: firefox 127.0.2.0 - Critical severity, chrome 129.0.6668.90 - High severity, openssl 3.3.0.0 - High severity, windows_10 10.0.19045.4894 - High severity, office 16.0.17830.20210 - High severity, and 1 High severity software - Details not provided.

Activity 2 : Copilot for Security Standalone Experience

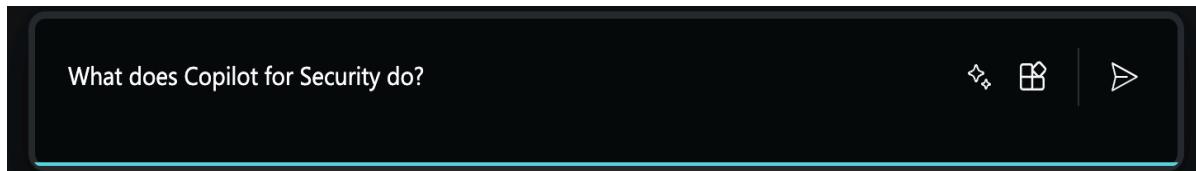
In this exercise, you will explore the Copilot for Security Standalone Experience. You will learn how to navigate the portal, manage plugins, and utilize various features to enhance your security operations. This hands-on activity will help you become familiar with the capabilities of Copilot for Security and how to effectively use it in your security workflows.

Explore Copilot for Security Standalone Experience

1. Open your browser, and go to the Copilot for [Security Standalone Portal](#)
2. Select the  **home menu** in the left corner
 - a **My session's** view on past sessions you created
 - b **Account** Ensure that you are signed in with your Alpine Ski house account. If it shows a different account, you need to sign out and sign in with the correct account.
 - c **Settings** include theme, time zone, and language preferences along with some settings for Copilot owners.

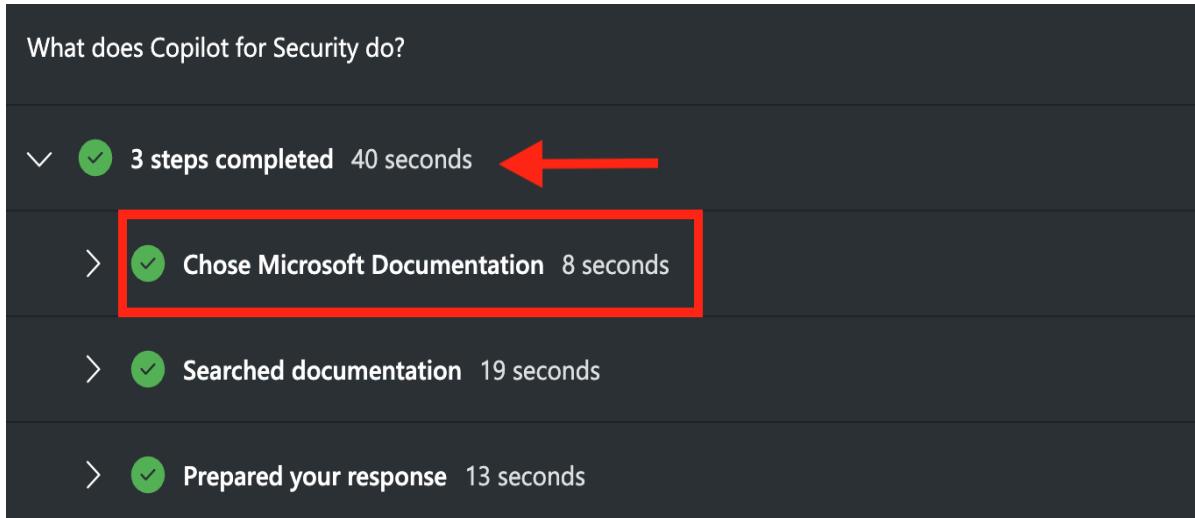
⚠️ Important Remark: *Since your account has the contributor role in Alpine Ski House, not all options are visible. Owners can manage capacity, data evaluation, see usage and more.*

3. You will find the **prompt bar** at the bottom of the Copilot home page. To ensure everything is working correctly, you can use a test prompt: **What does Copilot for Security do?**



4. Select **Send**  or press Enter. Wait for Copilot for Security to generate a response.
5. **Expand Steps Completed.**

💡 Tip: Notice the plugin selected was 'Microsoft Documentation' by the Copilot for Security Orchestrator. Microsoft Copilot orchestrator works behind the scenes to select and execute the right plugin and skill(s).



6. At any time during a Copilot for Security session, you can share your session with users in the same tenants. Select  Share to create a link.
7. The icon  in the prompt bar is used to manage **plugins**. You can toggle plugins on or off and configure them. We will get into more details later.

Tip: Plugins extend Copilot's capabilities by integrating with various security products from Microsoft or third-party providers. Think of Microsoft Copilot for Security like a smartphone, and the plugins are the apps you install to enhance its functionality.
8. Look for the sparkle icon  next to the prompt bar icon to use the search to find capabilities, also referred to as **skills**. Select **See all system capabilities** to see all the prompts listed for each plugin.

The screenshot shows a dark-themed interface with white text. At the top left is a menu icon (three horizontal lines) followed by the text "SYSTEM CAPABILITIES". To the right is a large red arrow pointing right, and next to it is the text "See all system capabilities >". Below this, a sub-section titled "Capabilities are based on the plugins you have set up." is shown. Underneath are four main sections: "Analyze a script or command", "Analyze security data", "Convert Unix Timestamp", and "Summary". Each section has a brief description below it.

- Analyze a script or command**
Analyze and interpret a command or script to natural language.
- Analyze security data**
Analyze, summarize, and explain security data such as event logs, and answer security questions.
- Convert Unix Timestamp**
Convert a Unix timestamp to a human readable date and time.
- Summary**

9. In the search bar, type **CVE** and reveal all the skill (set of function) that reside inside the Microsoft defender threat intelligence plugin.
10. Let's select "**Get CVE details by IDs**" and review the input that this skill required.

The screenshot shows a dark-themed interface with white text. At the top is a search bar containing the text "Get CVE details by IDs" with a close button. Below the search bar are two input fields: the first contains "CVE-2024-3400" and the second contains "Summary". At the bottom right is a blue "Run" button with a right-pointing arrow.

11. In the input parameter add the **CVE-2024-3400** and **Summary** press run.

Tip: By selecting the capability Copilot invoked the skill directly without using the Orchestrator.

12. Using the same sparkle icon, you can see a list of **promptbooks** that you can start with.

Tip: Promptbooks are collections of prompts designed to accomplish specific security tasks. They run a series of prompts in sequence, with each prompt building on the previous one.

The screenshot shows the Copilot for Security home page with a dark background. At the top is a search bar labeled "Search". Below it, a heading says "Get started using these examples". Under this, there's a section titled "PROMPTBOOKS" with a small icon of a document with a list. To the right of this section is a large red arrow pointing right, with the text "See all promptbooks >" next to it. Below the "PROMPTBOOKS" section, there's another example titled "Analyze Microsoft Sentinel Incident" with a brief description.

Get started using these examples

PROMPTBOOKS → See all promptbooks >

Promptbooks are sets of prompts that run in sequence automatically.

Analyze Microsoft Sentinel Incident

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

13. You can also select **View promptbook library** on the home page or via the settings menu. We will explore promptbooks in more depth later.

Manage Plugins

Copilot for Security comes with many preinstalled plugins available for Microsoft security services and other commonly used services and websites that you can use. You also have the option of extending default capabilities by adding your own custom plugins and non-Microsoft plugins as shown below:

1. The icon  in the prompt bar is used to **manage plugins**. You can toggle plugins on or off and configure them.
2. Select the plugin you'd like to use by turning the toggle on or off. For this lab make sure the **following plugins are toggled on:**
 - Microsoft Entra
 - Microsoft Defender XDR
 - Microsoft Defender Threat Intelligence
 - Microsoft Intune
 - Microsoft Purview
 - Microsoft Sentinel
 - Azure Firewall
 - Azure Web Application Firewall Preview
 - Natural language to KQL for Microsoft Defender XDR

💡 Tip: Copilot for Security some plugins need to be personalized by configuring the plugin setting. For example, for the Microsoft Sentinel plugin the default workspace needs to be provided. This has been already setup for the Alpine Ski house tenant.

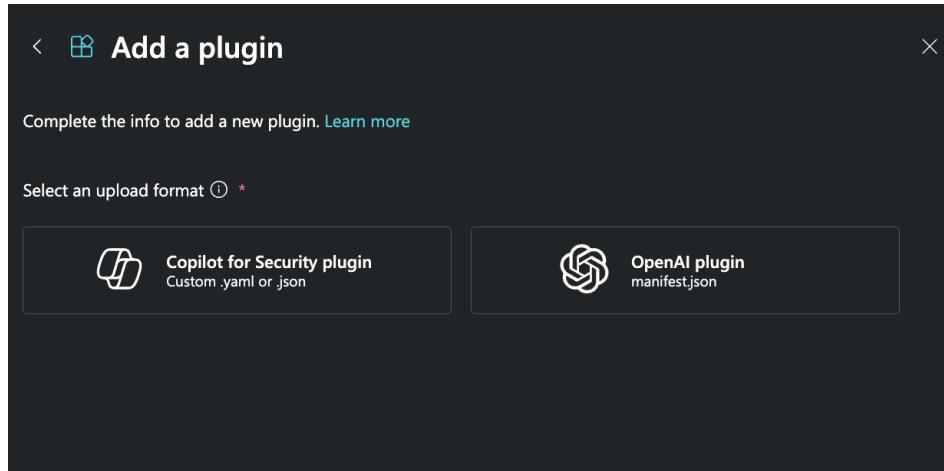
The screenshot shows the 'Manage sources' interface with the 'Plugins' tab selected. A search bar and filter buttons ('All (29)', 'On (10)', 'Off (19)') are at the top. Below is a list of Microsoft plugins, each with a toggle switch:

- Microsoft** (switch on)
- Microsoft Defender External Attack Surface Management** (switch on)
- Microsoft Defender Threat Intelligence** (switch on)
- Microsoft Defender XDR** (switch on)
- Microsoft Entra** (switch on)
- Microsoft Intune** (switch on)
- Microsoft Purview** (switch on)
- Microsoft Sentinel (Preview)** (switch on)

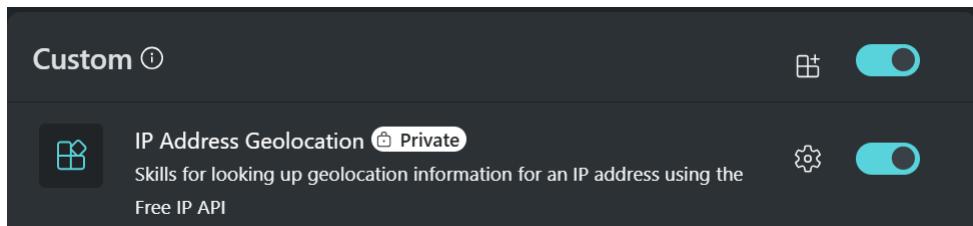
3. In Manage plugins, scroll down to the **Custom section**.
4. Select, **Add plugin**.

⚠️ Important Remark: This option is available because the Owner has configured Copilot for Security to allow Contributors to add and manage custom plugins for everyone in the organization. The custom plugin will be available to just yourself. Owners can decide to upload a plugin for themselves or anyone in the organization.

5. From the drop-down options, choose between adding a **Copilot for Security plugin or an OpenAI plugin**.
6. Depending on the plugin you'd like to add choose **to upload a file or upload as a link**. Select "API-GeoLocate.yaml" (Trainer to provide file location) from the "Lab Material" Folder.



7. After the plugin is successfully added, some plugins might need to be set up. You can also choose to set up the plugin later.



8. In the upcoming exercises we will configure a custom plugin.

Activity 3: Prompting Use Cases

Estimated time to complete this activity

Exercise 1: Effective Prompting

In this lab, we will practice creating effective prompts for Microsoft Copilot for Security. A prompt is the text you type to instruct Copilot on what you need. The quality of the response from Copilot largely depends on how clear and specific your prompt is.

 **Tip:** for Prompts! Good input = good output. Imagine you are instructing a junior security assistant. The more specific you are, the better they can help you.



Effective vs non effective prompts

In this exercise, you will learn the difference between ineffective and effective prompting by comparing two different approaches to querying information. You will also learn about common issues and mistakes when prompting Copilot for Security. Understanding these mistakes will help you and your team craft more effective prompts and get better responses from Copilot.

SESSION CONFUSION

Ineffective Prompt

1. Start a new session and in the prompt bar type, **Tell me about Defender incident 928** . Wait for Copilot for Security to generate a response.
2. Without starting a new session, use the same session to enter the prompt: **Tell me about Defender incident 751**
3. Without starting a new session, use the same prompt bar to enter the prompt: **Show me the audit logs for the incident**
4. Review the generated response and observe it's not clear which audit log the entries pertain to.

 **Tip:** *It's good practice to start a new session for each new topic or incident. This approach keeps the conversation clear and focused on the specific issue, avoiding confusion with previous topics.*

THREAT ACTOR INVESTIGATION

Ineffective Prompt

1. Start a new session and in the prompt bar type, **Tell me about Ruby Sleet**. Wait for Copilot for Security to generate a response.
2. Expand steps completed and **review the selected plugin**. Notice Copilot couldn't find a plugin by the Copilot for Security Orchestrator or selected Entra as a plugin.

 **Important Remark:** *Failing to provide necessary context or details, without specifying that Ruby Sleet is a threat actor or specifying the source will not result in a response.*

Note: *We continuously enhance our capabilities, including parallel processing and support for open prompts, to deliver high-quality responses to users. These improvements lead to even better results, and you may notice some activity in the lab as well.*

The image contains two side-by-side screenshots of the Copilot for Security interface.

Screenshot 1 (Left): The prompt "Tell me about Ruby Sleet" is entered. A red box highlights the "2 steps completed 7 seconds" message. Below it, the steps are listed: "Couldn't find a plugin for that" (3 seconds) and "Prepared your response" (5 seconds). The timestamp is Aug 26, 6:26 PM. A note says: "I'm sorry, but I don't have any information about 'Ruby Sleet'. Could you please provide more context or details? For example, is 'Ruby Sleet' a person, a software, a code name, or something else? This will help me provide a more accurate response." At the bottom, there's a "How's this response?" button and a scroll bar.

Screenshot 2 (Right): The same prompt is entered again. The "3 steps completed 6 seconds" message is shown. The steps are: "Chose Microsoft Entra" (4 seconds), "Processed your request" (1 second), and "Prepared your response" (2 seconds). The timestamp is Oct 16, 11:40 AM. A note says: "No data found for the given parameters. Please check input or consider rephrasing." There is also a small blue profile icon in the top right corner.

Effective Prompt

1. Without starting a new session type, **Tell me about threat actor Ruby Sleet**. Wait for Copilot for Security to generate a response.
2. Expand steps completed and **review the selected plugin**. Notice that Copilot has now selected the **Microsoft Threat Intelligence plugin** and provided an answer.

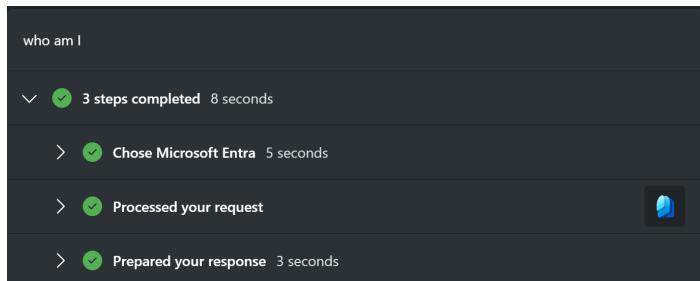
DISABLED PLUGIN

Ineffective Prompt

1. Click the icon  in the prompt bar used to **manage plugins**.
2. Toggle the Microsoft **Entra plugin off**.
3. Start a new session and in the prompt bar type, **Who am I**
- 4.

Effective Prompt

1. Click the icon  in the prompt bar used to **manage plugins**.
2. Toggle the Microsoft **Entra plugin on**.
3. Without starting a new session, use the same prompt bar to enter the same prompt: **Who am I**
4. Notice that Copilot has now selected the Microsoft Entra Plugin and provided an answer.



 **Tip:** If Copilot is unable to provide an answer, consider that the required plugin might be disabled. Check the plugin management settings to ensure that the necessary plugin is toggled on.

LONG AND COMPLICATED PROMPTS or GPT Token limits

Ineffective Prompts

1. Start a new session and in the prompt bar type, **Could you provide a detailed analysis of all security incidents from Microsoft Defender XDR over the past year? Please include insights on user activities, device logs, and network traffic associated with these incidents** Wait for Copilot for Security to generate a response.

Could you provide a detailed analysis of all security incidents from Microsoft Defender XDR over the past year? Please include insights on user activities, device logs, and network traffic associated with these incidents

>  Chose Natural language to KQL for Microsoft Defender XDR 6 seconds

<  Couldn't complete your request 25 seconds

The generated KQL query is not semantically or syntactically valid

GPT response was truncated with previous maxTokens threshold of 800. Retrying with maxTokens = 4096

Completion succeeded on retry of 901 tokens with increased maxTokens limit = 4096 Skill Name: GenerateKustoQuery Usage: Usage { PromptTokens = 16187, CompletionTokens = 901, TotalTokens = 17088 }. Output=To address this request, we need to perform a comprehensive analysis of security incidents from Microsoft Defender XDR over the past year. This involves querying multiple tables to gather data on incidents, user activities, device logs, and network traffic. We will also need to summarize the incidents by severity, resolution status, and identify common threat types. Finally, we will compare our findings to industry averages and provide recommendations for improving security posture.

⚠️ Important Remark: Large language models (LLMs) including GPT have limits on how much information they can process at once. This limit is known as a "[token limit](#)" and we reached that limit in this prompt.

- Copilot for Security can process prompt with multiple questions in prompt is structured and well written, Sample Prompt: **I'm interested in gaining insights into our Microsoft Defender incidents. Could you provide a summary of the total incidents from the last quarter, including a breakdown by severity and the current resolution status? Additionally, please identify the most common types of threats we faced and how our incident statistics compare to industry averages. Considering our current situation, do you believe we are prepared for future threats? What factors contribute to your assessment? Lastly, what changes should we consider to enhance our security posture?** Wait for Copilot for Security to generate a response

I'm interested in gaining insights into our Microsoft Defender incidents. Could you provide a summary of the total incidents from the last quarter, including a breakdown by severity and the current resolution status? Additionally, please identify the most common types of threats we faced and how our incident statistics compare to industry averages. Considering our current situation, do you believe we are prepared for future threats? What factors contribute to your assessment? Lastly, what changes should we consider to enhance our security posture?

> 3 steps completed 22 seconds

Oct 16, 12:10 PM

Summary of Microsoft Defender Incidents (Last Quarter)

Total Incidents

- Total Incidents: 118,156

Breakdown by Severity

- High Severity: 3
- Medium Severity: 7
- Low Severity: 0

Current Resolution Status

- Active: 10
- Resolved: 0
- In Progress: 0

Most Common Types of Threats

- Suspicious login from known IOC involving one user
- Suspected brute-force attack attempt involving multiple users
- Persistence incident involving multiple users
- Multiple failed user logon attempts to a service involving one user

Sample Incidents

- Incident: TI map IP entity to DNS on one endpoint
 - Severity: Medium
 - Status: Active
 - URL: <https://security.microsoft.com/incidents/182260?tid=536279f6-15cc->

I'm interested in gaining insights into our Microsoft Defender incidents. Could you provide a summary of the total incidents from the last quarter, including a breakdown by severity and the current resolution status? Additionally, please identify the most common types of threats we faced and how our incident statistics compare to industry averages. Considering our current situation, do you believe we are prepared for future threats? What factors contribute to your assessment? Lastly, what changes should we consider to enhance our security posture?

> 3 steps completed 17 seconds

Oct 16, 11:57 AM

Summary of Microsoft Defender Incidents (Last Quarter)

Total Incidents

- Total Incidents: 1459

Severity Breakdown

Severity	Count
High	6
Medium	4
Informational	1

Resolution Status

Status	Count
Active	9
Resolved	1

Common Types of Threats

- Multi-stage incidents involving Initial access & Lateral movement
- Exfiltration incidents
- DLP policy matches
- Automated investigations

Sample Incidents

⚠ Important Remark: *Using long and complicated prompts that are poorly structured and contain multiple questions can make it difficult for Copilot to interpret them effectively*

1. Start a new session and in the prompt bar type, **list all users and format as a table**
2. Notice that copilot truncated the response: *This table contains a subset of xx out of xxx records.*

The screenshot shows a Copilot session interface. At the top, the prompt is "list all users and format as a table". Below the prompt, a summary says "3 steps completed 13 seconds". The steps are: "Chose Microsoft Entra 5 seconds", "Processed your request 1 second", and "Prepared your response 7 seconds". The timestamp "Oct 17, 6:05 AM" is shown. A "Export to Excel" button is available. The main area displays a table with four rows of user data:

Display Name	User Principal Name	Email
u1046	u1046@ash.alpineskihouse.co	u1046@ash.alpineskihouse.co
u493	u493@ash.alpineskihouse.co	u493@ash.alpineskihouse.co
u2337	u2337@ash.alpineskihouse.co	u2337@ash.alpineskihouse.co

A note at the bottom states: "This table contains a subset of 10 out of 2823 records. To verify this information in the Microsoft Entra portal, you can navigate to the [User Management page](#) and search for these users."

⚠ Important Remark: *Response too long for the model to process in a single turn, can exceed the token size of the model and result in a truncated answer. For more detailed information on GPT token size limits, you can refer to [What are tokens and how to count them? | OpenAI Help Center](#)*

1. Start a new session and in the prompt bar type, **Show high severity defender incidents detected over the last year and summarize the trends**

It's likely that you will not get a useful answer for these types of trend prompts, because any outcome is just accidental, not intentional.

⚠️ Important Remark: *Currently, Copilot does not have the capability to analyze trends. Trend analysis is done by GPT, which isn't ideal for this task due to its limitations such as token size.*

Building and iterating on your prompt

This exercise focuses on building and iterating your prompts to create effective queries for Copilot for Security.

1. Start a new session and in the prompt bar type **Give me a summary of Defender incident 889**. Specifying the source can help get more accurate responses. Additionally, In real life a customer might have multiple incident systems.
2. Now further iterating, we can add the needed incident details. **Give me a summary of Defender incident 889 and list the entities involved.**
3. Being specific about the format and focus of your request can make the response better suited to your needs. **Give me a summary of Defender incident 889 and list the entities involved. Compile the information in a table and add a summary.**
1. By Tailoring the information to your audience, you can effectively communicate complex incident details in a way that is accessible and understandable to everyone. **Give me a summary of Defender incident 889 and list the entities involved. Compile the information in a table and start with a summary for a non technical audience.**

 **Tip:** *It's important to note that crafting the perfect prompt often takes a few iterations, and that's perfectly okay. You don't need to have a long, detailed prompt right from the start. Instead, you can break it down into multiple separate prompts and refine it as you go.*

Sample complex prompts with output

Prompt: Could you provide a bulleted list of the top 20 most critical Defender incidents from the past 30 days? Group these incidents by the analyst assigned to each one. For ease of access, include the reference number for each incident in the response. Also, could you include the median time taken to resolve these incidents? Additionally, exclude any incidents that are currently unassigned

Could you provide a bulleted list of the top 20 most critical Defender incidents from the past 30 days? Group these incidents by the analyst assigned to each one. For ease of access, include the reference number for each incident in the response. Also, could you include the median time taken to resolve these incidents? Additionally, exclude any incidents that are currently unassigned.

>  3 steps completed 20 seconds

Oct 16, 12:31 PM

Top 20 Most Critical Defender Incidents (Past 30 Days)

Grouped by Analyst Assigned

- **Mimik Emails - AlpineSkiHouse**
 - **Incident 2219:** Multi-stage incident involving Initial access & Lateral movement on multiple endpoints reported by multiple sources
 - **Incident 2563:** Multi-stage incident involving Initial access & Lateral movement including Ransomware on multiple endpoints reported by multiple sources
 - **Incident 2152:** Attack using AiTM phishing (attack disruption)
 - **Incident 2516:** Attack using AiTM phishing (attack disruption)
 - **Incident 2000:** Multi-stage incident involving Initial access & Lateral movement on one endpoint reported by multiple sources
 - **Incident 1972:** BEC financial fraud attack was launched from a compromised account (attack disruption)
 - **Incident 1914:** Multi-stage incident involving Execution & Lateral movement on multiple endpoints reported by multiple sources

Prompt: Please provide a comprehensive analysis of my current security posture using the Microsoft Defender XDR. This should include an overview of the current security status, an in-depth analysis of potential vulnerabilities, information about any active threats, a summary of recent security events, and recommendations for improving the security posture. Write a report for a non-technical audience in a clear and concise manner, with a focus on the most critical issues and recommendations.

Please provide a comprehensive analysis of my current security posture using the Microsoft Defender XDR. This should include an overview of the current security status, an in-depth analysis of potential vulnerabilities, information about any active threats, a summary of recent security events, and recommendations for improving the security posture. Write a report for a non-technical audience in a clear and concise manner, with a focus on the most critical issues and recommendations.

>  2 steps completed 19 seconds

Oct 16, 1:50 PM

Comprehensive Analysis of Current Security Posture Using Microsoft Defender XDR

Overview of Current Security Status

Your current security status, as monitored by Microsoft Defender XDR, indicates a mix of resolved and active incidents. The system has detected various types of threats, including ransomware, phishing, and unauthorized access attempts. The overall security posture shows that while many threats are being managed effectively, there are areas that require immediate attention to enhance protection.

In-Depth Analysis of Potential Vulnerabilities

- **User Activities:** There have been multiple incidents involving user accounts, such as unauthorized access attempts and phishing attacks. This highlights the need for stronger user authentication measures and regular security awareness training.
- **Device Logs:** Analysis of device logs reveals several instances of malware detection and suspicious activities. Ensuring that all devices are regularly updated and scanned for vulnerabilities is crucial.
- **Network Traffic:** The network traffic analysis shows attempts of lateral movement and data exfiltration. Implementing advanced network monitoring and segmentation can help in early detection and prevention of such activities.

Information About Active Threats

- **Ransomware:** There are ongoing incidents involving ransomware attacks. These attacks can lead to significant data loss and operational disruption if not contained promptly.
- **Phishing:** Phishing remains a prevalent threat, with several incidents reported involving attempts

Activity 4: Investigate an identity-based security incident.

In this exercise, you will investigate a potential identity-based security incident. You have received an alert indicating suspicious activity from a user account irvins@vnevado.alpineskihouse.co that has been flagged as a risky user.

Investigate in standalone

1. As a security analyst at Alpine Skihouse, you start a new session to investigate a specific user. You type: **Tell me about Entra user [irvins@vnevado.alpineskihouse.co](#)** in the prompt bar.
2. Copilot provides you with basic information about the user, including their role. You decide to dig deeper into the user's risk profile.
3. You type: **What is the risk level, state, and risk details for the above user?** Copilot responds with a detailed overview of risky activities associated with the user.
4. Next, you want to know about the user's recent sign-in activities. You type: **When did the above user last sign in, and to what target application?** Copilot provides the last sign-in time and the application accessed, giving you insight into the user's recent behavior.
5. To understand the user's security setup, you type: **What authentication methods are set up for the above user?** Copilot lists the authentication methods, such as multi-factor authentication (MFA) or password less sign-in, that are configured for the user. In lab, you might get insufficient permissions message.
6. You then check for any failed sign-in attempts. You type: **Did the above user have any failed sign-ins during the last 60 days?** If yes, list the location and IP address of each failed sign-in attempt." Copilot provides a list of failed sign-ins, including the locations and IP addresses, helping you identify any unusual patterns.
7. To complete your investigation, you need to review the user's audit logs. You type: **Show audit logs for the above user for the last 30 days.** Copilot generates a summary of the audit logs, detailing the user's activities and any significant events.

Using Copilot for Security, you gathered comprehensive information about the user, including sign-in activities, audit logs, and risky user detections.

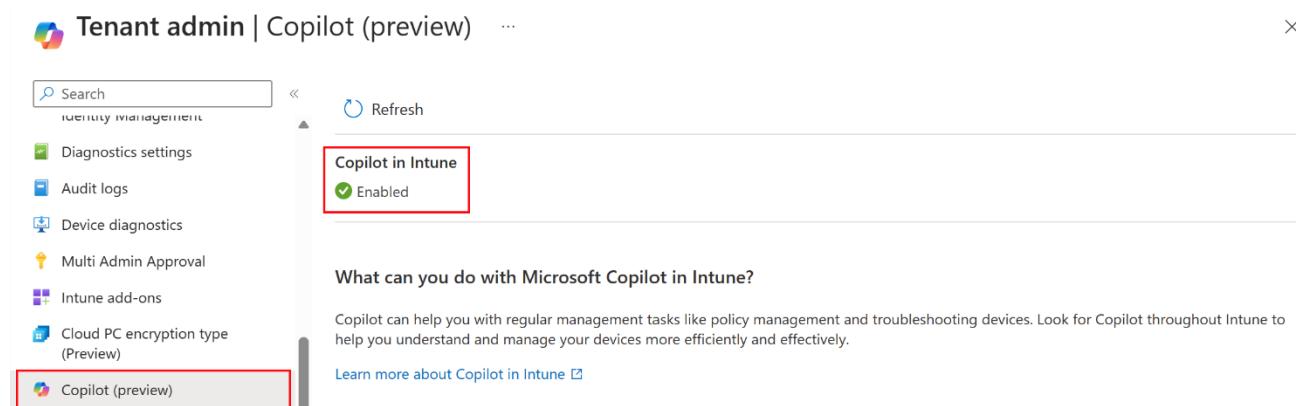
8. After completing your investigation, a Tier 2 analyst needs to take action to remediate or unblock the risky user. In the same session, you type: **Write a report based on this investigation. Provide your assessment of the user's risk level with supporting evidence and confidence level. List the most notable facts from this session as bullet points, along with supporting reasons. The audience is a Tier 2 SOC analyst who needs to take action to remediate or unblock the risky user. Include recommendations on how to proceed with user risk remediation in Entra.**

Activity 5: Intune

This exercise will give you a hands-on experience with the current Copilot for Security features embedded in the Intune portal. Copilot technology assists the device administrator in areas like managing policies and settings, understanding security posture, and troubleshooting of device issues.

⚠ Important Remark: Before you can use the Copilot features in Intune, Microsoft Copilot for Security must be configured, and you must complete the first run tour in the [Microsoft Copilot for Security portal](#). For the setup tasks, see [Get started with Microsoft Copilot](#). Due to the nature of this lab, you will not be able to experience the “first run tour”, but please familiarize yourself with bellow location to guide customers to the correct location to check that Copilot features has been enabled for Intune in their tenant.

Using your Apline Skihouse account, access [Intune admin center](#) > **Tenant administration** > **Copilot**.



The screenshot shows the Microsoft Intune admin center interface. At the top, there's a navigation bar with 'Search' and 'Identity management'. Below it is a sidebar with icons for 'Diagnostics settings', 'Audit logs', 'Device diagnostics', 'Multi Admin Approval', 'Intune add-ons', 'Cloud PC encryption type (Preview)', and 'Copilot (preview)'. The main area has a heading 'Copilot in Intune' with a green checkmark and the word 'Enabled'. Below this, a section titled 'What can you do with Microsoft Copilot in Intune?' explains that Copilot can help with management tasks like policy management and troubleshooting. At the bottom of the main content area, there's a link 'Learn more about Copilot in Intune'.

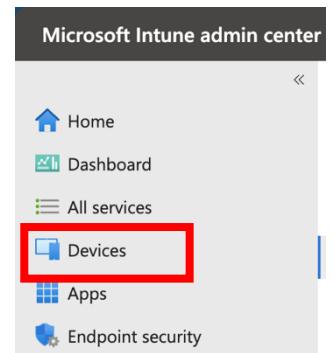
Intune Policy Management

The case:

You are an IT admin responsible for ensuring that the Intune environment has the right set of policies required for device management in the environment. You are required to manage and maintain the current set of policies. There is a new task at hand to deliver a new Windows compliance policy. Hence – you need to quickly get up to speed on creating a Windows compliance policy, learn which settings to deliver, ensure there are no conflicts and figure out the recommended values for the various settings.

⚠ Important Remark: Alpine Skihouse is a shared environment. Do not assign test-policies to any devices or users or groups, do not deploy your work to the tenant in the "review & create" guided wizard by using the "Create" button in the last step!

1. Go to **Intune admin center** > select “**Devices**” in left menu in the [Intune Admin Center](#)
2. In the horizontal menu “**Manage devices by platform**”, select Windows.
3. Go to **Manage Devices** > **Compliance**
4. In the top menu, select “**+Create Policy**”
5. Select platform “**Windows 10 and later**” > click “**Create**” button



6. Provide a name for the policy (just some random characters - non PII data) > click “**Next**”
7. Unfold “**Device Health**” and select the Copilot icon right next to “**BitLocker**”
8. Copilot provides a description of the setting, as well as any relevant sources, supporting your work as you are defining Windows compliance settings for your organization.
9. But importantly, you need to know if this specific compliance setting has been configured in any other policies!

Create a policy

Platform

Select platform

Windows 10 and later

Windows 8.1 and later

Device Health

Microsoft Attestation Service evaluation settings

Use these settings to confirm that a device has protective mea

Windows 10 and 11

BitLocker Require

Tell me about Intune setting "BitLocker"

Fetched Document Summary

The “BitLocker” setting in the “DeviceHealth” category for the “Windows 10/11 compliance policy” on the “Windows 10 and later” platform is related to the BitLocker Drive Encryption feature in Windows. BitLocker helps protect the data on the device’s operating system volume against unauthorized access and offline attacks.

Here are some key points from the fetched documents:

- BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted

10. Click the "**book symbol**" to see suggested prompts in the guide and explore further.
11. Select "**Has this setting been configured in any other policies?**"

Please note that the "BitLocker" setting in Intune is not required by default, meaning it can be configured based on the organization's security requirements.

Sources:

- [1]: Device Compliance settings for Windows 10/11 in Intune ↗
- [2]: BitLocker and policy settings compliance ↗
- [3]: BitLocker-encrypted Windows 10 device shows as Not compliant in Intune ↗
- [4]: BitLocker settings reference ↗

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

How could this setting affect users? 

Does Microsoft recommend any particular value for this setting? 

Generated by Copilot for Security ↗ Learn more ↗

Prompt guide

Tell me about Intune setting "BitLocker"

Has this setting been configured in any other policies?

Does Microsoft recommend any particular value for this setting?

How could this setting affect users?

How could this setting affect security?

Does Microsoft recommend any particular value for this setting? 

12. Copilot helps you and finds any potential conflicting policies that include the same settings.

Has this setting been configured in any other policies?

The 'BitLocker' setting, which is part of the 'DeviceHealth' category for the 'Windows 10/11 compliance policy' on the 'Windows 10 and later' platform, is indeed configured in one of your existing policies. Here are the details of the policy:

- **Policy Id:** 22fc6a93-3336-4fc1-ab09-73abc2eb5092
- **Policy Name:** Device Risk

13. Just for good measures, you ask Copilot for Microsoft's recommendations for the setting you are configuring – **select “Does Microsoft recommend any particular value for this setting”** at the suggested prompts right next to the “book” icon.
14. (Feel free to test out the other suggested prompts, before you continue the lab exercises)

Does Microsoft recommend any particular value for this setting?

Based on the fetched documents, the setting “BitLocker” under the “DeviceHealth” category for the “Windows 10/11 compliance policy” on the “Windows 10 and later” platform is not explicitly discussed. However, there are some general recommendations and practices related to BitLocker settings in the context of device compliance and security:

- In the context of device health, BitLocker is often used to encrypt

⚠ Important Remark: Remember to NOT deploy your work to the tenant, **exit out** e.g. click “Devices Overview” in the path-menu – then select “OK” in the pop-up! (thank you)

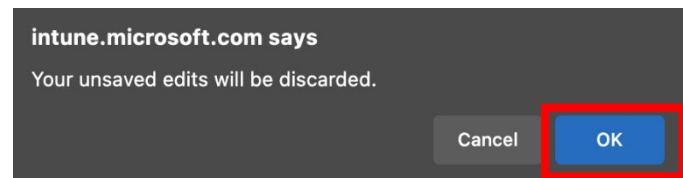
Home > Devices | Overview > Windows | Compliance >
Windows 10/11 compliance policy ...
Windows 10 and later

Basics 2 Compliance settings 3 Actions for noncompl

Custom Compliance

Device Health

Microsoft Attestation Service evaluation settings
Use these settings to confirm that a device has protective measures



Intune Summarize Existing Policies and Assess Their Impact to Users and Security

You are a new IT admin that is tasked with reviewing and delivering a security policy for your environment encompassing BitLocker, ASR and more. You have inherited the role from another admin and were informed that some policies have already been created. You need to be able to summarize the existing policy, and learn of its impact on users and security, prior to creating new ones or editing existing ones.

1. Go to **Intune admin center** > select “**Devices**” in left menu in the [Intune Admin Center](#)
2. In the horizontal menu “**Manage devices by platform**”, select Windows.
3. Go to **Manage Devices** > **Configuration**
4. Select the “**Enhanced Antiphishing**” configuration policy
5. Select “**Summarize with Copilot**” – and you get an easy way to determine what the policy is meant to configure.

The screenshot shows the Intune Admin Center interface. At the top, there's a breadcrumb navigation: Home > Devices | Configuration >. Below it, a card titled "Enhanced Antiphishing" (Device configuration profile) has a red box around the "Summarize with Copilot" button. To the right, a callout box says "Summarize this policy". The main content area shows "Device and user check-in status" with a bar chart where "Succeeded" is 31 and others are 0. A "View report" button is below. A sidebar box titled "Device assignment status" says: "This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state." To the right, a detailed description of the policy settings follows:

The policy in question is named "Enhanced Antiphishing". It has several settings configured, which are as follows:

1. **Automatic Data Collection (Windows Insiders only)**: This setting is enabled and it allows for automatic collection of website or app content when additional analysis is needed to help identify security threats. Please note that this setting is only available to Windows Insiders.
2. **Notify Malicious**: This setting is enabled and it configures Enhanced Phishing Protection notifications for malicious content.
3. **Notify Password Reuse**: This setting is enabled and it configures Enhanced Phishing Protection notifications for protecting passwords from reuse.
4. **Notify Unsafe App**: This setting is enabled and it configures Enhanced Phishing Protection notifications for protecting passwords typed into M365 Office applications, Notepad, and Wordpad.
5. **Service Enabled**: This setting is enabled and it enables Enhanced Phishing Protection in audit mode for Windows 11 H2.

6. But – you obviously need to get a better understanding of the user impact from the settings inside the policy. As in the previous Intune exercise, have a look and try the suggested prompts next to the “**book icon**”

Describe the impact of this policy on users

Describe the impact of this policy on security



(Graphics intentionally left out) – Please take a closer look at the Copilot results, select “**Describe the impact of this policy on users**” and Select “**Describe the impact of this policy on security**”

Describe the impact of this policy on users

Describe the impact of this policy on security

Implementing the **Enhanced Antiphishing** policy will have the following impacts on users:

1. **Automatic Data Collection (Windows Insiders only):** Users who are part of the Windows Insider program will experience automatic collection of website or app content when additional analysis is needed to identify security threats. This could raise privacy concerns among users who are aware of the data collection.
2. **Notify Malicious:** Users will receive notifications when malicious content is detected. This will enhance their awareness of potential threats but may also lead to alert fatigue if notifications are frequent.
3. **Notify Password Reuse:** Users will be notified if they reuse passwords, which helps in maintaining better password hygiene. However, this might be seen as intrusive by some users who prefer to manage their passwords independently.
4. **Notify Unsafe App:** Users will receive notifications when they type passwords into unsafe applications like Notepad, Wordpad, or M365 Office applications. This will help in preventing credential theft but could be perceived as annoying if users frequently use these applications.
5. **Service Enabled:** Enhanced Phishing Protection will be enabled in audit mode for Windows 11 H2 meaning users will not

Implementing the **Enhanced Antiphishing** policy will have a significant impact on security by enhancing phishing protection and user awareness of potential threats. Here are the key security impacts:

1. **Automatic Data Collection (Windows Insiders only):** This setting allows for the automatic collection of website or app content for additional analysis to identify security threats. While this enhances security by providing more data for threat detection, it could potentially impact user privacy and system performance due to the collection and processing of large amounts of data.
2. **Notify Malicious:** This setting configures notifications for malicious content, which will alert users to potential threats. This proactive approach helps in preventing security breaches by making users aware of malicious activities in real-time.
3. **Notify Password Reuse:** By notifying users when they reuse passwords, this setting helps in maintaining better password hygiene, reducing the risk of credential theft and unauthorized access.
4. **Notify Unsafe App:** This setting provides notifications when passwords are typed into unsafe applications like Notepad, Wordpad, or M365 Office applications. It helps in preventing credential theft by alerting users to potential phishing threats. However, frequent notifications could lead to alert fatigue, potentially causing users to ignore important warnings.
5. **Service Enabled:** Enabling Enhanced Phishing Protection in audit mode for Windows 11 H2 helps in identifying potential phishing threats without blocking user activity. This provides valuable information for assessing and improving security

Assistance to troubleshoot devices in Intune, using Copilot for Security.

Now you are a helpdesk admin tasked with troubleshooting devices in Intune. You are facing a situation where policies and apps are missing from one device but are showing up on another device. You need to quickly understand more about the devices and compare them for apps and policies.

1. Go to **Intune admin center** > select “**Devices**” in left menu in the [Intune Admin Center](#)
2. In the horizontal menu “**Manage devices by platform**”, select Windows.
3. In the Device overview, use the Search field and type: **CPC-u123-MCMLHU**
4. Click on the Device name itself

Home > Devices | Overview >

Windows | Windows devices

Search: CPC-u123-MCMLHU

Device name	Managed by	Ownership
CPC-u123-MCM	Intune	Corporate

5. To get a quick overview of the device itself, you can use Copilot for Security features, click “Explore with Copilot” or “Explore Device”

Home > Devices | Overview > Windows | Windows devices >

CPC-u123-MCMLHU

...   Sync Restart

Overview 

Manage  Properties  Monitor

Essentials 

Ready to explore this device? Copilot can provide AI-generated insights to help you troubleshoot.

Summarize this device 

Analyze an error code

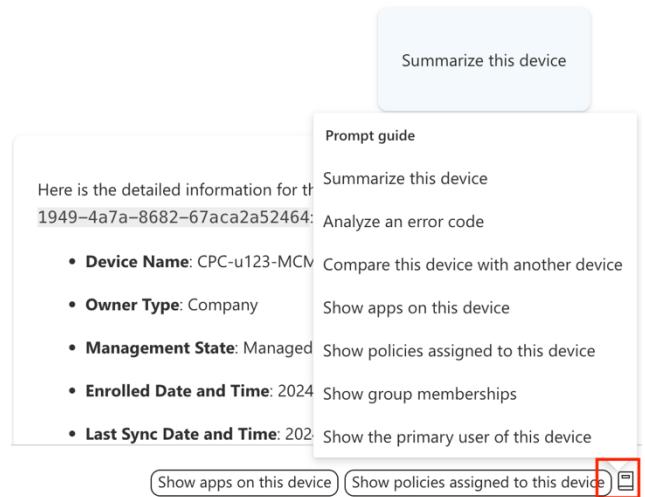
Compare this device with another device

Show apps on this device

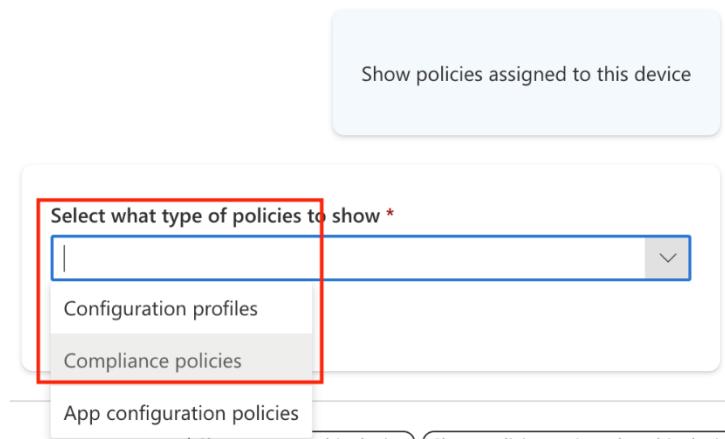
Show policies assigned to this device

6. You are now presented with a range of **this** options to explore the device with assistance. Choose "**Summarize device**" to get a more in-depth presentation of key stats of the device.

7. Try to scroll down through all parts of the Summary, Copilot collects a lot of different insights about the device - saving you time to fetch them in different locations of the Intune portal. Next, try to click the “**book icon**” again, and you see a list of suggested prompts to continue your analysis of the device.



8. Obviously, you noticed that the device was not compliant! – To understand why and get further details, select the suggested prompt “**Show policies assigned to this device**”.
9. A new menu pops up, select “**Compliance policies**”



10. You quickly get a complete list of the assigned policies and their status. Hence you can determine what made the device non-compliant and investigate in Intune why said policy has not applied or is not working on the device.

The device CPC-u123-MCMLHU with id 6d9d0270-2e61-4d5c-975a-fb570cbf5d2c has 2 compliance policies assigned to it. Here are the details:

PolicyId	PolicyName	PolicyStatus
c0f4911a-7ce6-4804-8563-677a2665d379	Default Device Compliance Policy	Compliant
22fc6a93-3336-4fc1-ab09-73abc2eb5092	Device Risk	Not compliant

The user associated with this device is u123@a.alpineskihouse.co. The device last contacted the server on 2024-08-28 20:59:55.000000.

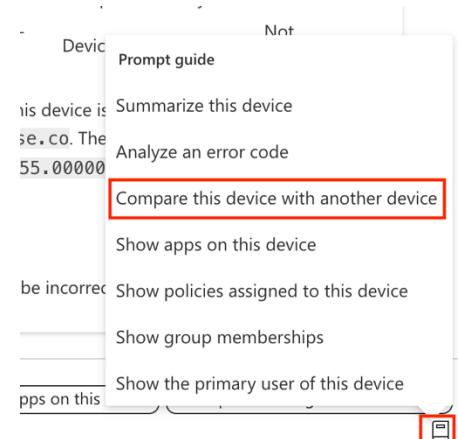
 **Tip:** Stay at current view after step 10 above, next exercise continues from same place.

Compare devices for troubleshooting

A common troubleshooting scenario stems from users reporting e.g. missing apps, missing settings that gives a certain user experience etc. – the users experience the lack of something on their devices, or they realize their device is not configured in the same way as their peer's devices.

A quick way to try figure out why **Device A** is misconfigured or lacks some apps, is to compare it to a known correctly working device – **Device B**. Copilot for Security makes it much easier to compare two devices, instead of doing this by hand manually and collecting different stats about the devices at different places in the Intune portal.

1. Return to the screen from step 10 in the previous exercise and click the book icon.
2. Select “**Compare this device with another device**”.



3. For Device 2 fill in “**VNEVADO-Win10B**”. Select the Comparison type drop down and select “**Managed apps**”, hit Submit.
4. Try to revert to step 1 of this exercise and Compare devices again – this time select “Configuration Policies”. Observe the rich details of differences.

Select another device and what you want to compare

Device 2 *	<input type="text" value="VNEVADO-Win10B"/>
Comparison type *	<input type="text" value="Managed apps"/>
<input type="button" value="Submit"/>	

The device CPC-u123-MCMLHU has a total of 4 managed apps, while the device VNEVADO-Win10B has a total of 6 managed apps.

The device CPC-u123-MCMLHU has no unique managed apps. However, the device VNEVADO-Win10B has 2 unique managed apps. Here are the details:

Application	Version	Resolved Intent	Installation Status
Microsoft 365 Apps for Windows 10 and later		requiredInstall	Installed
Microsoft Edge for Windows 10 and later	128.0.2739.54	requiredInstall	Installed

CPC-u123-MCMLHU differences:

PolicyName	PolicyStatus	UPN
Default Tamper Protection Policy	Succeeded	System account
Default Antivirus Policy	Succeeded	System account
Defender for Endpoint onboarding	Succeeded	u123@alpineskihouse.co

VNEVADO-Win10B differences:

PolicyName	PolicyStatus	UPN
Firefox extensions	Error	System account
Chrome extensions	Succeeded	System account
Purview Edge browser extension	Succeeded	System account
MDE Tamper Protection off	Succeeded	System account
MDAV not configured	Succeeded	System account
OneDrive	Succeeded	nestorw@vnevado.alpineskihouse.co

Analyzing error code in Intune

As you were checking up on Irvin's Windows device, your eyes zoomed in on an error!! Copilot for Security to the rescue – follow the steps and try out how.

1. Jump back to the overview of Windows devices.
2. Search for the device named "**ASH-IrvinS1**", in the list click the device name (in blue)
3. On the new left-side menu, select "**Device Configuration**" and find the error message at the "**Firefox extensions**" policy – BAM! Good thing your keen eyes found that error! Now click on the Firefox extensions to read out the error code.

Enhanced Antiphishing	System account	Settings Catalog	Succeeded
Firefox extensions	System account	Device configuration	Error
Firewall Exception for Azure Bastion	u293@ash.alpineskihouse.co	Microsoft Defender Firewall Rules	Succeeded

4. You can use both error codes, the results will be the same when Copilot analyses them, copy one of them to your clip board.

The screenshot shows the "Firefox extensions" policy details. On the left, there's a table with columns for "Source Profile" (Source Profile) and "Error code" (-2016281112). On the right, there's a "SOURCE PROFILES" section listing "Source Profile" and "Firefox extensions". Below that is an "ERROR CODE" section with the value "0x87d1fde8".

5. Now jump back to the device "**ASH-IrvinS1**" overview page and invoke the "**Explorer with Copilot**" once more.
6. This time, from the different suggested prompts, select "**Analyze an error code**"

The screenshot shows a form titled "Analyze an error code". It has a text input field labeled "Enter an error code to analyze." containing the value "-2016281112". Below the input field is a "Submit" button.

7. Paste in the error code and hit "Submit"

8. From the rich results you now know exactly what that error code means, and you can continue your work and correct the error.

The error code -2016281112 or 0x87D1FDE8 corresponds to "Remediation failed" [1]. This error can occur in different scenarios.

In the context of Microsoft Intune, this error can occur when you deploy a Managed Browser policy. Specifically, if you deploy the "Configure URLs that will be allowed or blocked in the Managed

9. This concludes the short exercise; above picture is only a snippet of the full response.

Activity 6 Purview: Investigate a data leakage (DLP) incident

You start your day as a security analyst at Alpine Skihouse, ready to tackle the latest data loss prevention (DLP) alerts. Your first task is to identify the top DLP alerts for today. Data Loss Prevention (DLP) is a feature within Microsoft Purview that helps prevent sensitive information from being shared or exposed accidentally.

Investigate in standalone

- As a security analyst at Alpine Skihouse, you start your day by identifying the top DLP alerts. You open the Copilot for Security Standalone Portal and type: **What are the top DLP high severity alerts?**

The screenshot shows a dark-themed interface for the Copilot for Security Standalone Portal. At the top, a search bar contains the query "What are the top DLP high severity alerts?". Below it, a progress indicator shows "3 steps completed 23 seconds". The timestamp "Sep 5, 3:39 PM" is displayed. A message says "Displaying top 2 Microsoft Purview Data Loss Prevention (DLP) alerts with 'High' severity:". On the right, there are "Export to Excel" and "Copy" buttons. A table lists two alerts:

Alert ID	Alert Title	Severity
dl146bf2fa-7b13-ae61-2e00-08dccc0326d7	DLP policy (U.S. Financial Data) matched for email with subject (Document)	High
dl146bf2fa-7b13-ae61-be00-08dccc8955b0	DLP policy (U.S. Financial Data) matched for email with subject (The numbers you need)	High

- One alert stands out: an email with the subject "The numbers you need" has triggered a DLP policy match for U.S. Financial Data. You type: **Tell me more about the alert 'DLP policy (U.S. Financial Data) matched for email with subject (Document)'.** Copilot provides details about the policy.
- Next, you want to know more about the file involved. You type: **What are the details of the file involved in this alert?** Copilot responds with specifics about the file.

4. Concerned about the potential risk, you investigate the user. You type: **Tell me about the user risk associated with this alert.** Copilot provides an insider risk assessment.
5. To get a complete picture, you also need information about the device used. You type: **Tell me more about the device used in this alert.** Copilot responds with device details.
6. Finally, you check if this user has had any risky sign-ins in the past 30 days. You type: **Has this user had any risky sign-ins in the past 30 days?** Copilot provides a summary of the user's sign-in activities.
7. With all this information, you need to summarize your findings into an email. You type:
Summarize all of the above into an email. Please include information about the user including location, job title, their manager name and manager email. Provide the findings of this session and provide me some recommendations on next steps. Copilot generates a comprehensive email.

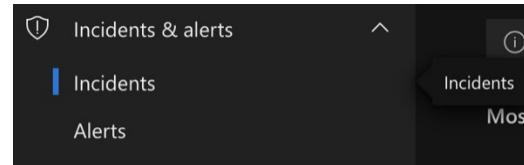
⚠️ Important Remark: *By summarizing Insider Risk Management alerts in Purview Embedded, you can gather a lot of information with less capacity unit usage. See [Exercise 3: Purview](#)*

Exercise 4: Investigate BEC Fraud Attack incident

This exercise involves investigating a **Business Email Compromise (BEC) fraud attack** using Microsoft Defender and Copilot for Security. You'll search for the incident, review the summary, identify involved entities, check the reputational score of a malicious IP, assess the impact on devices and users, compile a report summarizing your findings and recommendations, and finally, save the prompts in a promptbook.

Incident Summary

1. Go to **Investigation & response > Incidents & alerts > Incidents on** in the [Microsoft Defender portal](#)
2. On the left side of the screen, select "**Incidents**"



3. In the incident search bar, start typing "**BEC financial fraud attack was launched**" and hit enter. Select Incident ID: **483** if available

The screenshot shows the search results for the query "BEC financial fraud a...". The results table includes columns for Incident name, Incident Id, Tags, and Severity. One result is shown: "BEC financial fraud attack was launched from a co... 483 BEC Fraud +4 High".

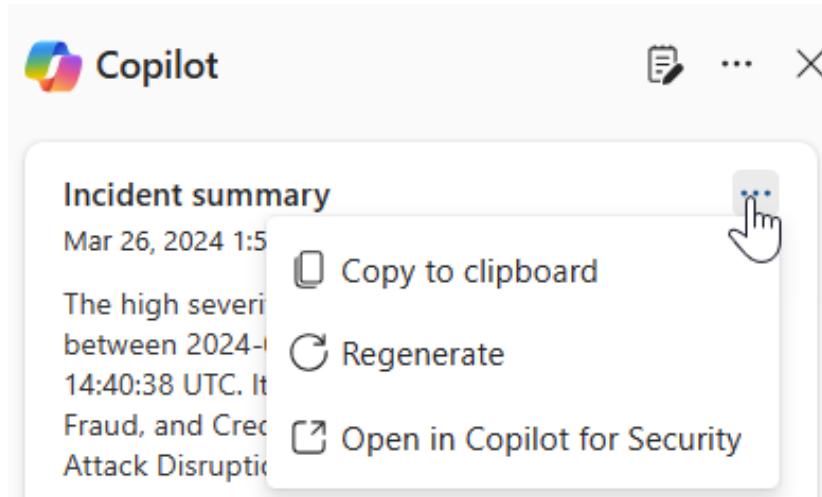
Incident name	Incident Id	Tags	Severity
BEC financial fraud attack was launched from a co...	483	BEC Fraud +4	High

4. Open the incident page by clicking on it >Copilot automatically creates an incident summary upon opening the page. **Review the generated summary as it maps the information to Kill chain.**

 **Tip:** When you open an incident page, Copilot immediately summarizes an incident's most valuable information to help you quickly assess the incident status and risk in order to take the first action immediately.

Continue the incident investigation in the standalone portal

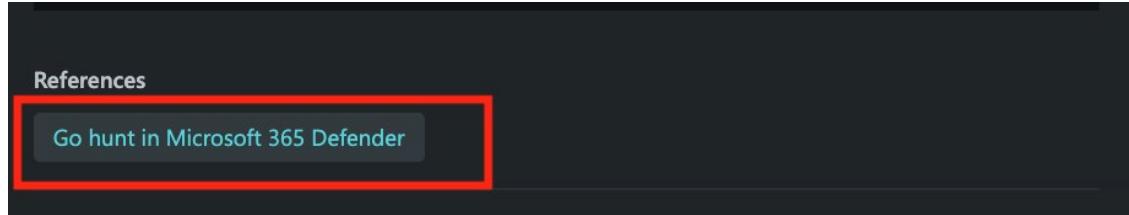
5. Select the More actions ellipsis (...) at the top of the incident summary > **Selecting Open in Copilot for Security** opens a new tab to the Copilot for Security standalone portal.



6. In the prompt bar type, **Can you extract any indicators of compromise and entities from the incident?** Wait for Copilot to generate a response.
7. As an experienced security analyst, we know that once we have 3 types of entities (user, host, IP), we have different pivoting options, let's start with a follow up question about that remote IP, and ask **What is known about the reputation of the malicious ip address?**

 **Tip:** Review the chosen plugin and note the response; reputational score and justification.
8. After we understand that the IP is malicious with a score of 100, we want to look inside the organization and understand the blast radius of the impact on the user and the host. **What devices are associated with the user mentioned in the incident? Can you check if those devices are compliant? Format the results as a table, for devices that are not compliant, summarize the steps required to make device or device compliant.**

 **Tip:** Review the chosen plugin and note the response; reason for non compliance.
9. Let's focus on the involved user and check if it the user appears in other alerts. **Hunt across Defender 365 to see if this user is associated with any other alerts**
10. The expectation is that the NL2KQL plugin searches the AlertEvidence Table and that the user is associated with multiple alerts. Now click **Go hunt in Microsoft 365 Defender**.



11. Now verify and **run the KQL query**

```
1 AlertEvidence
2 | where AccountName == 'leeg'
```

12. Switch back to your session in standalone.

1.

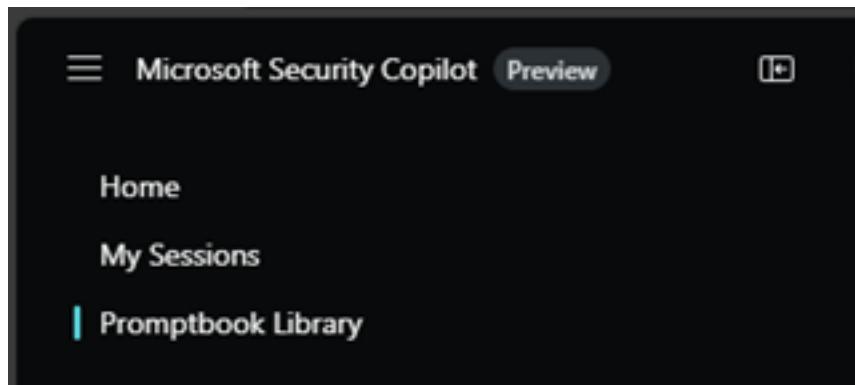
13. As we are ending our shift, we have to pass on or transfer the case to another analyst, so we want copilot to assist us in condensing all the crucial steps of our investigation. **Write a report based on this investigation. Lead with your assessment of the incident and supporting evidence for your conclusion with a confidence level, including whether or not this incident is likely to be a true positive. Conclude with a set of recommendations and next steps.**

Create a promptbook from your session

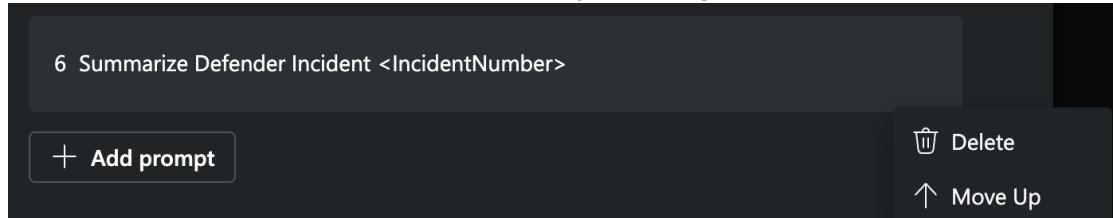
14. These investigation steps and the prompts used, can help us with similar incidents, so we will **save them in a promptbook**. To do that, we need to check the box above and click the icon above.



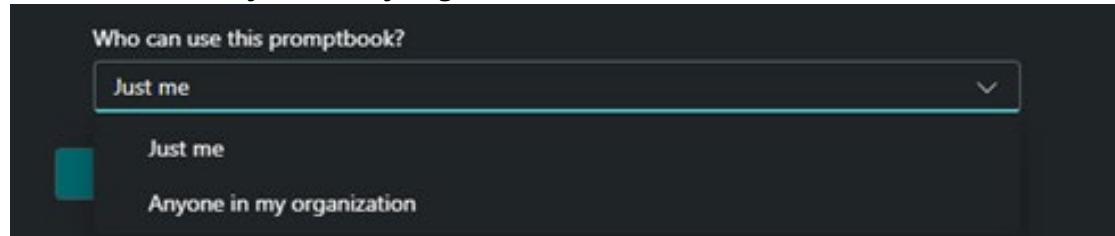
15. Promptbooks can accept input parameters, and in our case the **dynamic parameter** will be the Defender incident number that we enter in the first prompt. Give a descriptive name for the prompts book (add your name to it) and hit **Save**.
16. Both prebuilt and user-built promptbooks across your organization appear in the promptbook library. View the promptbooks by going to the Copilot menu and selecting **Promptbook Library**.



17. The promptbook library displays all the promptbooks available to you. **Select the Promptbook you just created > click to Open > select Edit**  in the upper right.
18. Scroll Down and Click **Add Prompt**. In this example we want incident number as required input, **<IncidentNumber>** or any easily understood parameter name as long as you **use angle brackets <>** and **no spaces** to define it.
19. Move the new prompt to the first position by selecting **Move Up**.



20. You can then define if this promptbook can be used only by you (**Just me**) or if you would like to share it (**Anyone in my organization**). Select **Just Me**.



21. Save your Promptbook. In the Promptbook Run page, insert the required parameter (incident number 483) that you set earlier and select **Run**.

Activity 7: Extensibility

Estimated time to complete this activity

120 minutes

Objectives

Extensibility is to enable participants to explore and understand the extensibility features of Microsoft Copilot for Security. Participants will learn how to integrate and manage custom plugins, configure plugin settings, and extend the capabilities of Copilot for Security by adding new functionalities such as knowledge base integration. This activity aims to provide hands-on experience by leveraging the extensibility options available in Copilot for Security.

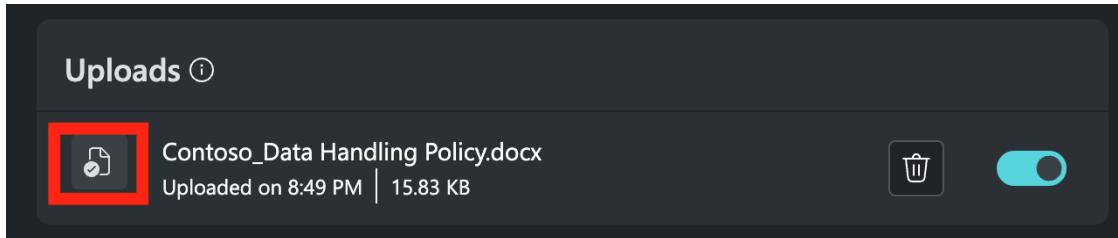
Exercise 1: Knowledge Base Integration

In this exercise, you will upload a file in Microsoft Copilot for Security to allow Copilot to refer to the contents of the file. This allows Copilot to reason over the knowledge base or documents and generate responses that are more relevant, specific, and customized to your operational needs.

File Upload

1. Use Contoso_Data Handling Policy.docx to an accessible location.
2. In the Copilot home page, select the sources icon  in the prompt bar to open the **Manage sources** page.
3. Select **Files** to open the file upload section.
4. Select **Upload file** to look for your file.
5. Wait for the file to appear in **Uploads** with a check. If an error message appears, correct the problem and try again.)

⚠️ Important Remark: *Uploaded files are only available to the user account that uploaded them, and not available to other users within or outside the tenant.*



Using the uploaded Policy document in Copilot for Security

1. Start a new session and in the prompt bar type, **Summarize Defender incident 107**. Wait for Copilot to generate a response.
2. Then type, **list any actions taken by the user that may violate the Data Handling Policy in my uploaded files. Format the response leading with a verdict on if the actions violate any policies and include confidence. Cite the policy name and section applicable to the verdict.**

Based on the analysis of the user's actions in relation to the "Contoso Data Handling Policy", Copilot should outline several potential policy violations.

Review Azure AI Search in Copilot for Security

Since this environment isn't set up for Azure AI Search, we will not configure this plugin, only review it. Configuring involves, entering the required information, including the search instance name, index name, vector field, text field, title field, and API key.

1. Select the Copilot sources icon  in the prompt bar.
2. Go to **Microsoft > Azure AI search** and select **Set up**.

 **Tip:** The Azure AI Search plugin connects to an index accessible to the entire organization, in contrast to file upload only available to individual users. The prompting experience is similar to file upload. Instead of referring to uploaded files, you would refer to 'Azure AI Search' in your prompt.

Exercise 2: KQL Sentinel Cost Custom Plugin

This exercise demonstrates how to create a KQL plugin for Copilot for Security Custom Plugin using the example of a KQL query against the Usage table and providing valuable context. This includes explanations of Sentinel tables, detailed cost summaries, and cost-saving recommendations. This added context helps users better understand their Sentinel costs and optimize their security operations.

Configure and review the KQL Custom Plugin

1. **Download** [KQL-SentinelCost-Alpine-Ski.yaml](#) to an accessible location.
2. Open in your favorite editor and **review the settings of the yaml file**.

 **Tip:** *The YAML file is pre-populated with Alpine Ski House's Entra TenantId, SubscriptionId, ResourceGroupName, and WorkspaceName for the Sentinel instance. Normally, you would need to provide this information.*

3. **Review and run the query in Sentinel.** Navigate to your Microsoft Sentinel workspace in the Azure portal In the Sentinel workspace, go to the "Logs" section.
4. **Copy and paste the following KQL query into the query editor:**

```
let fromDateTime=datetime('June 01 2024');
let toDateTime=datetime('September 01 2024');

Usage
| where IsBillable == true
| where TimeGenerated between ( fromDateTime .. toDateTime )
| where DataType <> "AzureDiagnostics"
| summarize size = sum(Quantity)/1024, sizeOther =
sumif(Quantity,(DataType !contains "_CL" and TimeGenerated between
( fromDateTime .. toDateTime )))/1024 by DataType
| project ['Table Name'] = DataType, ['Table Size']=size,
['Estimated cost']=size*4.3
| order by ['Estimated cost'] desc
| take 20
```

5. Start a new session and in the prompt bar type. **Can you provide a detailed summary of the total of my Sentinel Costs of the past 90 days?**

⚠ Important Remark: It's expected that Copilot can't provide an answer at this stage as the plugin has not been added.

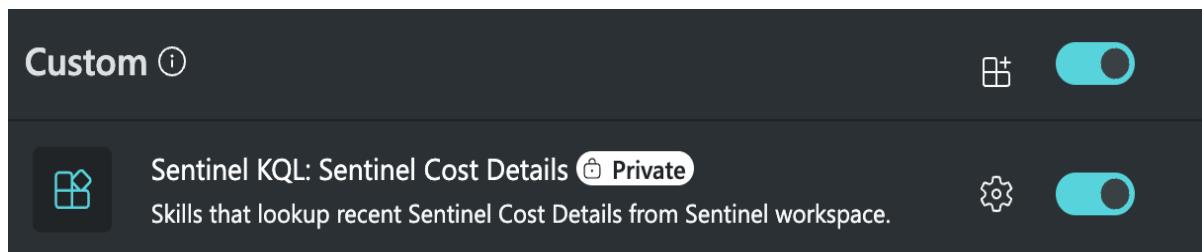
Can you provide a detailed summary of the total of my Sentinel Costs of the past 90 days?

✓ 2 steps completed 17 seconds

> ⓘ Couldn't find a plugin for that 12 seconds

> ✓ Prepared your response 6 seconds

6. Select the Copilot sources icon  in the prompt bar.
7. In Manage plugins, scroll down to the Custom section.
8. Select, **Add plugin**.
9. After the plugin is successfully added, your plugin will be visible in the Custom section. You can turn the toggle on or off.



⚠ Important Remark: Since your account has the contributor role in Alpine Ski House, the plugin is available to just yourself. Owners can decide to upload a plugin for themselves or anyone in the organization.

10. Look for the sparkle icon next to the prompt bar icon to use the search to find capabilities, also referred to as skills. Select **See all system capabilities** to see all the prompts listed for each plugin.

A screenshot of a search results page. The search bar at the top contains the text "Sentinel Cost". Below the search bar, there is a section titled "SYSTEM CAPABILITIES" with the sub-section "SENTINEL KQL: SENTINEL COST DETAILS". Underneath this, there is a heading "Get Sentinel Cost" followed by a description: "Fetches all the Sentinel Cost details for each table for the specified time and date range from Sentinel.".

11. In the search bar, type **Sentinel Cost** and reveal the custom plugin.

Using the plugin in Copilot for Security

1. In the prompt bar type. **Can you provide a detailed summary of the total of my Sentinel Costs of the past 90 days?**

🔍 **Tip:** It's now expected that Copilot can provide an answer now that the plugin is added.



⚠️ **Important Remark:** KQL plugins are using on behalf permissions. In this environment your account already has access to the Sentinel Workspace.

2. Let's iterate and add more context. **Provide a detailed summary of the total of my Sentinel Costs of the past 90 days. Outline for all tables what it is used for within Sentinel and the security value it provides, format as a table. Also total up all the cost to give me an average of monthly costs. Also be sure to give any costs savings recommendations based on my data ingestion.**
3. Lastly ask for recommendations. **How do my current data retention policies impact the costs of the largest table? Would adjusting these policies yield significant cost savings?**

🔍 **Tip:** This exercise aimed to demonstrate the extensibility value of plugins. While running a KQL query can be done directly in Sentinel, the true value lies in using Copilot for Security to take the data and add meaningful context, such as explaining Sentinel tables and providing cost-saving recommendations.

Exercise 3: Using KQL and API Plugins to investigate a custom GCP Log

In this exercise, you will analyze user activity involving user Chris S. You will investigate a GCP log that has been archived and stored on an ADX cluster. You will enable the ADX plugin in Copilot for Security, as well as a Shodan and GEO IP plugin, to gather more context around this investigation.

The purpose of this exercise is to demonstrate that Copilot for Security is an extensible platform capable of bringing extra knowledge to the table, such as understanding GCP logs. By following these steps, you will gain hands-on experience in analyzing a log using various plugins and generating a comprehensive report.

Configure and review the plugins

1. **Download** below plugins to an accessible location.

- API GEO IP Plugin: [API-GeoLocate.yaml](#)
- KQL-ADX-GCP Plugin: [KQL-ADX-GCP.yaml](#)

2. Open in your favorite editor and **review the settings of the yaml files**.

⚠ Important Remark: *API plugins, including the GEO IP plugin, typically require authentication to access their services. However, the GEO IP plugin is free and does not require any special authentication. Additionally, the OpenApiSpecUrl refers to a publicly available location containing the file with the actual API logic. The plugin file itself serves as a description of the plugin and provides instructions on how to use it within Copilot for Security.*

3. Open your browser, and go to the **Copilot for Security Standalone Portal**

4. Select the Copilot sources icon  in the prompt bar.

5. In Manage plugins, scroll down to the Custom section.

6. Select, **Add plugin API-Geolocate**

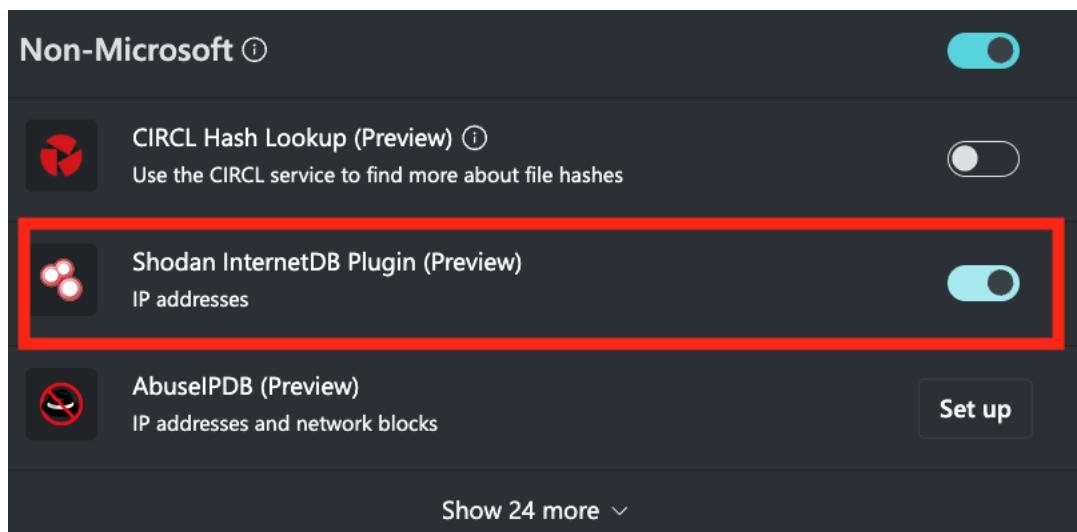
7. After the plugin is successfully added, your plugin will be visible in the Custom section. You can turn the toggle on or off.

8. Then do the **same for KQL-ADX-GCP**

9. Then again, the Copilot sources icon  in the prompt bar.

10. Scroll down to non-Microsoft and **toggle Shodan on**.

⚠ Important Remark: *The Shodan plugin requires an API key for authentication. However, the owner has configured the plugin settings in Copilot for Security to allow contributors to use the plugin without needing to provide their own API keys.*



11. Look for the sparkle icon next to the prompt bar icon to use the search to find capabilities, also referred to as skills. Select **See all system capabilities** to see all the prompts listed for each plugin.
12. In the search bar, type **Shodan** and verify that the plugin is available.
13. Repeat the process by searching for **GEO** and **GCP** to ensure that these plugins are also available.

Verify ADX cluster and query access

2. Open your web browser and go to the **Azure portal**
3. Sign in with your **Alpine Skihouse credentials**.
4. Once you're signed in, use the search bar at the top of the page and **type Azure Data Explorer or ADX**.
5. **Select Azure Data Explorer** from the search results. This will take you to the Azure Data Explorer blade.

6. In the Azure Data Explorer blade, you will see a list of your ADX clusters. Select the cluster **alipine-cluster01**.
7. Click on the **Query** button to open the query editor where you can start querying your data.
8. Run a simple query to verify access, such as **GCPAuditLogs** and hit the **Run** button.
9. If the query returns a list **results**, you have access to the ADX cluster.

Note: Lab account may not have access to ADX cluster in Azure Portal but this exercise can be used as a reference

The screenshot shows the Azure Data Explorer blade for the cluster 'alipine-cluster01'. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Data, Databases, and Query. The main area features a search bar, a 'Run' button, and a results pane. The results pane displays a single row of data: '1 GCPAuditLogs'. The 'DB01' database is selected in the tree view under 'alipine-cluster01.eastus/DB01'.

Using the plugins in Copilot for Security

2. In the prompt bar type. **Can you describe in detail over a few paragraphs the GCP Audit Log operations associated with officechris@gmail.com between July and August this year? Be sure to also include all the logs in a format I can export.**

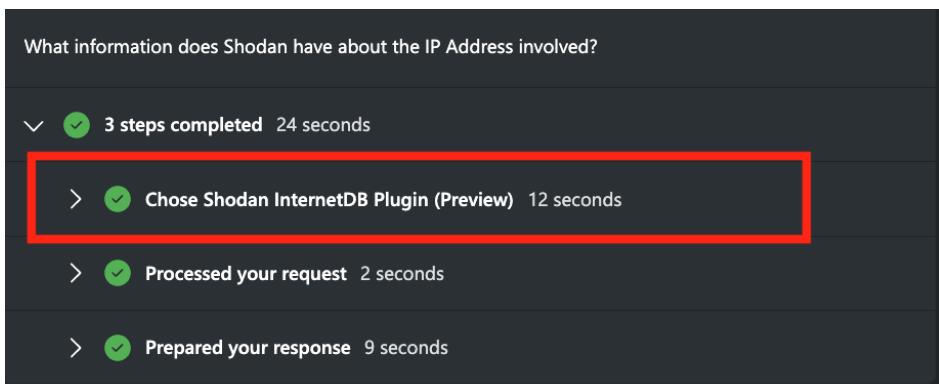


3. Continue your session with: **Compare the filter changes between the GCP log entries, what was changed? Why would a user make that change?**

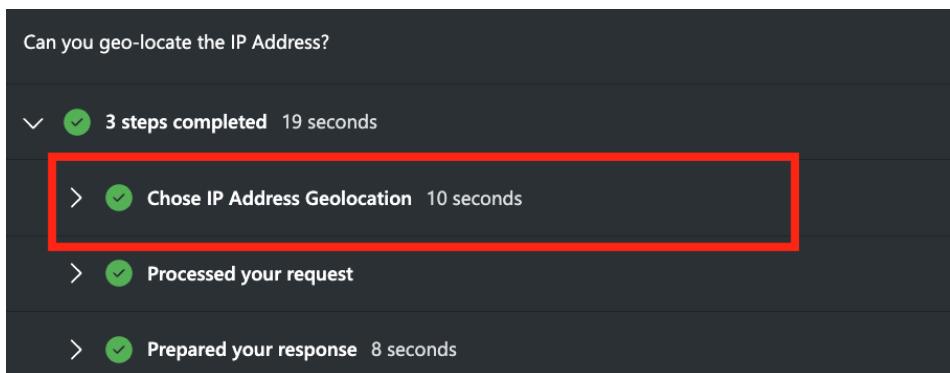
By using Copilot for Security, you were able to gather comprehensive information about the user activity in easy to understand language.

4. Research the IP mentioned in the log by asking:**What information does Shodan have about the IP Address involved?**

By combining plugins such as Shodan, it can help in understanding the context and vulnerabilities of the IP address involved in the investigation



5. Use another plugin to gather more information about the geographical location of the IP address by asking: **Can you geo-locate the IP Address?**



6. Close your investigation with a report by asking: **Write a report summarizing this investigation. Lead with a non-technical executive summary, followed by a detailed and descriptive summary over a few paragraphs detailing your understanding of all relevant events, critical entity and threat intelligence information followed by next steps for remediation.**

The report ensures that all stakeholders are informed about the investigation's outcomes and provides a structured approach to addressing any security concerns identified during the investigation.

 **Tip:** Storing log files on ADX is a common practice because it is cost-effective and allows for querying large volumes of data. Additionally, the KQL logic used in the GCP plugin is very similar to that used for other types of custom logs, making it easy to reuse.

Activity 4: Automation (Optional as do not have lab permissions)

Estimated time to complete this activity

45 minutes

Objectives

1. Learn how to manually configure an Azure Logic App.
2. Understand each component involved in the Logic App workflow.
3. Automate the retrieval and summarization of threat intelligence articles.
4. Send daily email bulletins with the summarized threat information.

Exercise 1: Create Threat Bulletin Logic App

This lab guides you through the process of manually configuring an Azure Logic App to automate the retrieval and summarization of the latest threat intelligence articles, and sends them as a daily email bulletin. Understanding the manual setup will provide deep insights into the configuration and functioning of the components in Azure Logic Apps.

Add a new Logic App

1. **Navigate to Logic Apps:** In the Azure Portal, search for "Logic Apps" in the search bar and select it.
2. **Create Logic App:** Click on the "+ Add" button to create a new Logic App.
3. Select hosting option **Consumption**.
4. **Fill in Details:**
 - Select the Subscription **M365_Infra** and Resource Group **Sentinel_Demo**.
 - Provide a **unique name for the Logic App**. Incorporate your initials and the current date in the name to ensure uniqueness. For example: PPM_ThreatBulletin_20240910.
 - Choose a **Region East US**
 - Set **Enable Log Analytics** to **No**.

5. Review and Create:

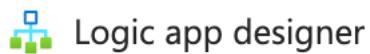
- After entering the details, click on **Review + create** to review the configuration.
- Once the review is complete, click on **Create** to finalize the creation of the Logic App.

Open the Logic App in Logic App Designer

6. After Azure successfully deploys your logic app resource, select **Go to resource**

7. **Select Development > Tools > Logic app designer.**

✓ Development Tools



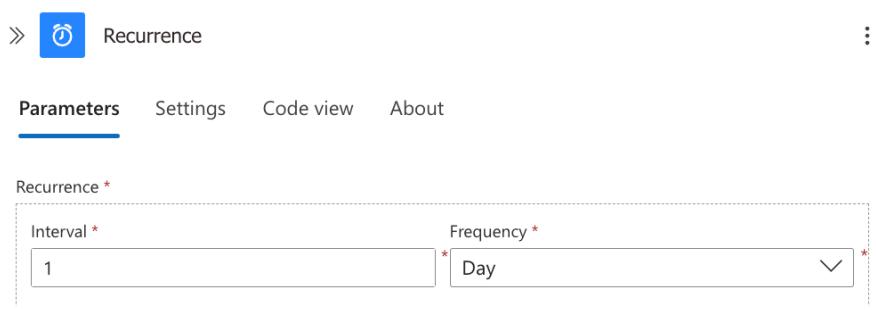
Add Actions

Once created, use the Logic App Designer to add triggers and actions based on your requirements. You will use connectors to integrate with various services and create workflows.



SETUP RECURRENCE TRIGGER

8. On the designer, select Add a trigger, if not already selected.
9. The **Add a trigger** pane opens and shows the available connectors that provide triggers,
10. Search for Recurrence and select the **Recurrence trigger**. Set the recurrence: **Frequency:**
 - **Day**
 - **Interval: 1**



GET THE LATEST THREAT ARTICLES

11. To add the action under the last step in the workflow, select **the plus sign (+)**, and then select **Add an action**.
12. The **Add an action** pane opens and shows the available connectors that provide actions. Search for **Copilot for Security** and select **Submit a Copilot for Security Prompt**.

Add an action

X

The screenshot shows the 'Add an action' interface. At the top, there is a search bar containing 'copilot for security'. Below it, there are two dropdown menus: 'Runtime' (set to 'Select a runtime') and 'Action type' (set to 'Actions'). A checkbox labeled 'Group by Connector' is checked. Below these, the 'Microsoft Copilot for Security' connector is listed with its icon. Two actions are shown: 'Run a Copilot for Security promptbook' and 'Submit a Copilot for Security prompt'. The second action, 'Submit a Copilot for Security prompt', is highlighted with a red border.

13. The Create connection screen appears, click Add New, click **Sign in**. Sign in with your **Alpine Skihouse account**.

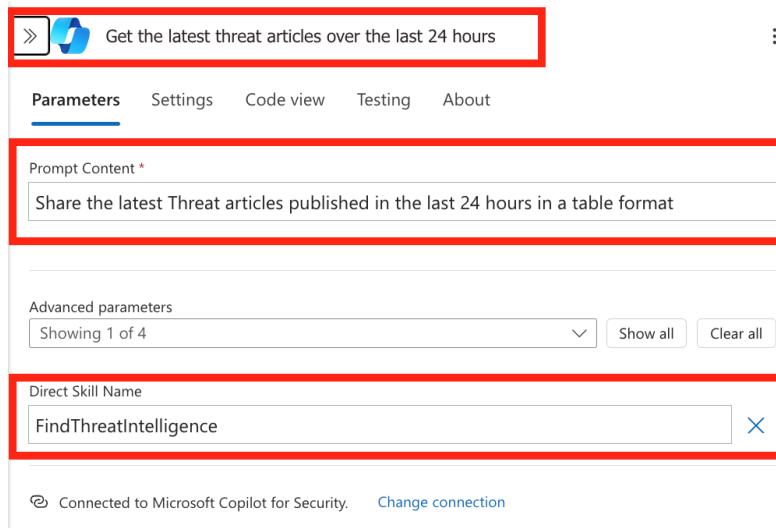
⚠️ Important Remark: If the login page doesn't appear. Close the create connection screen by clicking the "X" button located at the top-right corner and try again..

The screenshot shows the 'Create connection' interface. At the top, there is a search bar containing 'Submit a Copilot for Security prompt'. Below it, there is a section titled 'Create a new connection'. It includes fields for 'Authentication *' (set to 'OAuth') and 'Tenant ID *' (set to '(new) AlpineSkiHouse'). A note below says 'Sign in to create a connection to Microsoft Copilot for Security.' A 'Sign in' button is at the bottom.

⚠️ Important Remark: The connector operates using on behalf of the Entra (AAD) user with necessary permissions. This connection is not shareable, so if the Logic App is shared, users will need to create their own connection.

14. Configure the **action**:

- **Name:** Get the latest threat articles over the last 24 hours
- **Prompt content:** Share the latest Threat articles published in the last 24 hours in a table format
- **Advanced Parameters > Direct Skill Name:** FindThreatIntelligence



⚠️ Important Remark: Using the Direct Skill Name is a convenient and cost-effective method for triggering specific actions quickly and bypassing the orchestrator. However, it can sacrifice the session context that the orchestrator provides, which could be valuable for more complex, context-dependent tasks.

SUMMARIZE INTO A THREAT BULLETIN

15. To add the action under the last step in the workflow, select the **plus sign (+)**, and then select **Add an action**.
16. The Add an action pane opens and shows the available connectors that provide actions. Search for **Copilot for Security** and select **Submit a Copilot for Security Prompt**.
17. Configure the **action**:
 - **Name:** Summarize into a threat bulletin
 - **Prompt content:** /AskGPT Summarize the following articles and consolidate them in a Threat Bulletin format Named Threat bulletin with the current date . In the bulletin ensure to capture all details including the title summary , link , Created date , also highlight the action items the Team should prioritize in relation to these articles.

- **Advanced Parameters > [SessionId]**

The screenshot shows the Microsoft Copilot for Security interface. At the top, there's a blue icon with a lightning bolt. Below it, a red box highlights a skill icon with a blue and white design followed by the text "Summarize into a threat bulletin". Further down, a red box highlights the "Prompt Content" field, which contains the following text:
/AskGPT Summarize the following articles and consolidate them in a Threat Bulletin format Named Threat bulletin with the current date . In the bulletin ensure to capture all details including the title summary , link , Created date , also highlight the action items the Team should prioritize in relation to these articles.

Below this, there's a section for "Advanced parameters" with a dropdown showing "Showing 1 of 4" and buttons for "Show all" and "Clear all". A red box highlights the "SessionId" parameter input field, which contains "sessionid x". At the bottom, there's a note about being connected to Microsoft Copilot for Security and a "Change connection" link.

⚠️ Important Remark: Enter an existing Copilot sessionId for maintaining continuity in your tasks, allowing to ask prompts within the same investigation. If omitted, Copilot creates a new investigation. /AskGPT is used to call the skill directly, together with sessionId the context is maintained.

CREATE FILE

1. Click **New step**
18. To add the action under the last step in the workflow, select the plus sign (+), and then select **Add an action**.
19. The Add an action pane opens and shows the available connectors that provide actions. Search for **Create file** and select **OneDrive for Business**

The screenshot shows the "Add an action" pane. At the top, there's a "OneDrive for Business" connector icon. Below it, a red box highlights the "Create file" action, which is listed in the pane. There are also "See more" and "i" (info) buttons.

20. Create connection appears. **Sign in with your Alpine Ski house account (uxxxx@ash.alpineskihouse.co).**

21. Parameters:



Inputs > Dynamic Contents

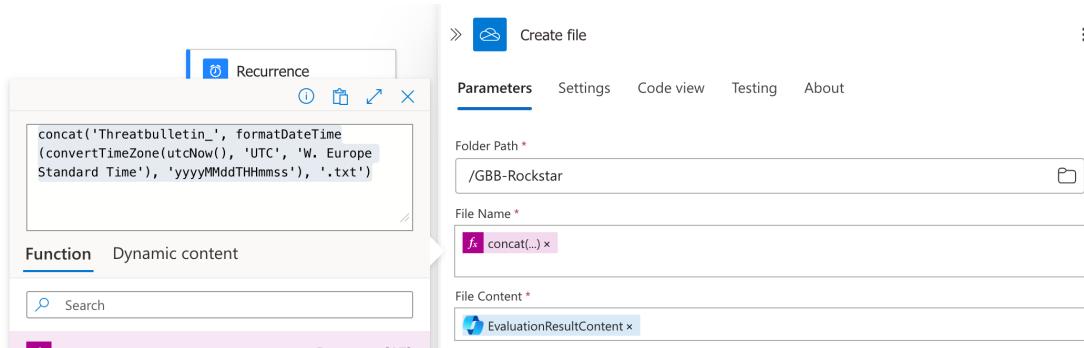
```
concat('Threatbulletin_', formatDateTime(convertTimeZone(utcNow(), 'UTC', 'W. Europe Standard Time'), 'yyyyMMddTHHmmss'), '.txt')
```

This function generates a filename by concatenating the string "Threatbulletin_" with the current date and time in the format yyyyMMddTHHmmss (adjusted to Western European Time), followed by the file extension ".txt". For example, it might produce a filename like "Threatbulletin_20240902T151942.txt".

- **Folder Path:** /GBB-Rockstar



- **File Content:** EvaluationResultContent



Save and Run the Logic App

Used Capacity Units: 0.81

⚠️ Important Remark: In addition to Standard Capacity Units (SCU), the cost for Logic Apps includes charges for triggers, actions, and connectors used in the workflow. These costs are based on the number of executions and the type of connectors (standard or enterprise) utilized.

1. Once all actions and connections are configured, click **Save**.
2. The Create connection screen appears, click **Sign in**.
3. Click **Run** to manually trigger the Logic App and ensure it works as intended.
4. Click on **Runs history** to see the status of each run and troubleshoot any issues that may arise.
5. Switch to Copilot for Security Standalone and note that under **my sessions**, a new session has been created.

Name	Last updated	Created
LogicApp: Share the latest Threat articles published in the last 24 hours in a table format	7:40 PM	7:40 PM

Tip: Now that you have successfully launched a Logic App utilizing the Copilot For Security connector review more samples available in our [public repository](#). These samples cover various security scenarios.

6. Go to [Sign in - Microsoft OneDrive \(live.com\)](#) and **Sign in with your Alpine Ski house account (uxxxx@ash.alpineskihouse.co)**.
7. The ThreatBulletin file should be there under My files/GBB-Rockstar

My files > GBB-Rockstar

Name
Threatbulletin_20240905T105539.txt

Clean up after usage

1. **Delete Logic App:** Navigate to the Logic App you created, click on **Delete** in the top menu, and confirm the deletion

