

Use promptbooks to save time

Build and utilize promptbooks to speed up your existing workflows



Promptbooks are a powerful tool for streamlining investigation flows and multi-step tasks. Promptbooks were designed to be run with a single click, saving users valuable time. Copilot includes many standard promptbooks for common task flows and users can also create/edit custom promptbooks.

Promptbook (noun)'prämp-,buk

A predefined set of prompts that automate common, repeatable workstreams.



Copilot includes built-in promptbooks that are ready to use out of the box



Suspicious script analysis

Get a report analyzing the intent, intelligence, threat actors, and impacts of a suspicious script.



Microsoft Defender incident investigation

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



Threat actor profile

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



Vulnerability impact assessment

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



Microsoft Sentinel Incident Investigation

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

Example promptbook flow:

Summarize Sentinel incident <SENTINEL_INCIDENT_ID>

Tell me about the entities associated with that incident.

What are the reputation scores for the IPv4 addresses on that incident?

Show the authentication methods setup for each user involved in that incident. Especially indicate whether they have MFA enabled.


If a user is listed in the incident details, show which devices they have used recently and indicate whether they are compliant with policies.

If any devices are listed in the previous output, show details from Intune on the one that checked in most recently. Especially indicate if it is current on all operating system updates.

Write an executive report summarizing this investigation. It should be suited for a non-technical audience.

How to build a promptbook

If you have a set of prompts that are frequently repeated, like an investigation or other task flow, creating a custom promptbook can be especially useful.

1. Find or **start a session** that you would like to turn into a promptbook.
2. **Select the prompts** that you would like to turn into a promptbook using the checkboxes on the left side of your screen
3. Click the  **“create promptbook”** icon at the top of the screen
4. The “Create a promptbook” window will appear, where you will create the name and description, edit your prompts if needed, and select who can use it (Just you or anyone in your organization)
5. **Click Create**

Create promptbook

Create a promptbook

Prompts

Add any inputs needed to each prompt. For example, if a prompt includes an incident ID, it should be entered in the prompt as <IncidentID>. Use angle brackets with no spaces.

Give me a profile summary of CVE <CVEID>.

If there are TI articles related to this CVE, provide a list and summary of them & include links.

If there were TI articles found, what recommendations does the first article in the list have for protecting against this CVE?

Summarize the CVE, associated threat actors and recommendation insights into an executive report. It should be suitable for a less technical audience.

+

Inputs you'll need

Inputs added to the prompts will be automatically displayed here. If you don't see the inputs, make sure the format is correct.

CVEID

Who can use this promptbook?

Just me

Create

Cancel

To see more and move faster, organizations need generative AI technology that complements human ingenuity and refocuses teams on what matters.

Microsoft Copilot for Security is a generative AI-powered assistant for daily operations in security and IT. Copilot empowers teams to protect at the speed and scale of AI by turning global threat intelligence, industry best practices, and organizations' security data into tailored insights to outsmart and outpace adversaries.

Learn more: <https://aka.ms/securitycopilot>

© Copyright Microsoft Corporation. All rights reserved.