Onboarding

The intention of this guide is focused on post-deployment activities. For a detailed deployment plan for onboarding Microsoft Security Copilot, please refer to the official documentation:

Get started with Microsoft Security Copilot Early Access Program
https://learn.microsoft.com/en-us/security-copilot/get-started-security-copilot

It includes a deployment process in three steps:
Step 1: Assign roles.
Step 2: Confirm your geography.
Step 3: Choose data sharing.

Foundation: plugin and use cases validation

Security Copilot uses on-behalf of authentication to access security related data through active Microsoft plugins. Specific Microsoft Entra roles and Azure RBAC roles must be assigned in order for a group or individual to access the Security Copilot platform. Once you're logged into the portal, your access determines what plugins are available to utilize.

Understand authentication in Security Copilot
https://learn.microsoft.com/en-us/security-copilot/authentication

Prompting and Sample Prompts

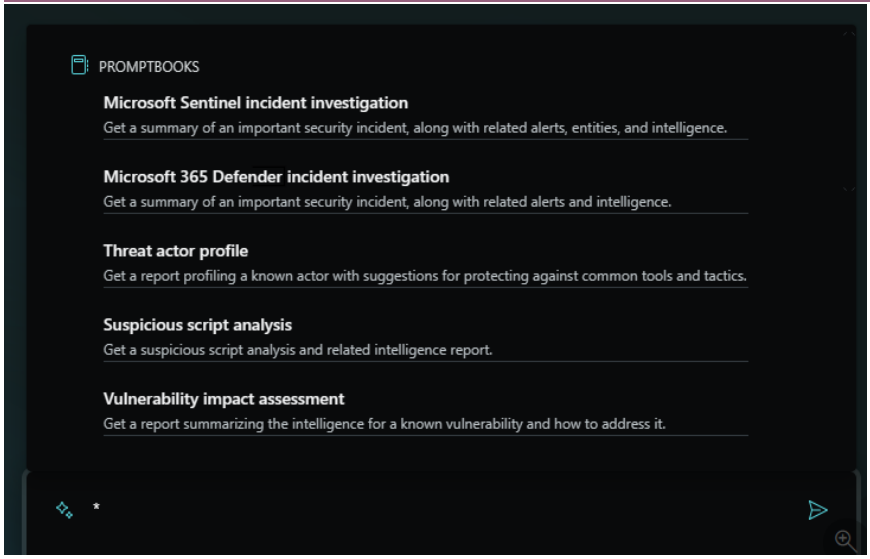
Watch the Security Copilot tour to get familiar with the standalone Security Copilot experience, if you haven't already.

Once you're all set up in Security Copilot, you can start using prompts. Prompts are the primary input Security Copilot needs to generate answers that can help you in your security-related tasks.

Here are some ways to interact with the standalone Security Copilot:

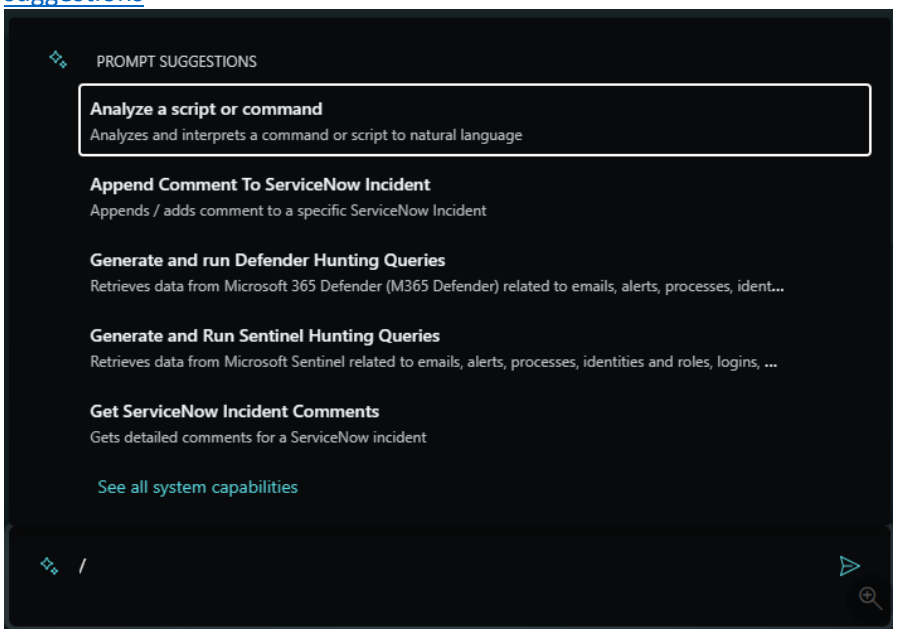
1. **Using promptbooks**

https://learn.microsoft.com/en-us/security-copilot/prompting-security-copilot#use-promptbooks



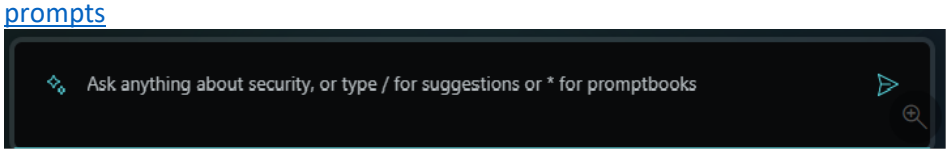
2. **Selecting from prompt suggestions**

https://learn.microsoft.com/en-us/security-copilot/prompting-security-copilot#select-from-prompt-suggestions



3. **Create your own prompts.**

https://learn.microsoft.com/en-us/security-copilot/prompting-security-copilot#create-your-own-prompts



Sample-Prompts

Entra

- Whoami
- What is the status of the user account for <**Username**>? Is it locked out?
- What login attempts exist for the user on December 31st? (Created KQL)
- What login attempts exist for the user in last 14 days? (Created KQL)
- What login attempts exist for the user <**UPN**> in last 14 days? (Targeting a specific user)
- Is the user considered risky? If so, why?
- Tell me more about <**user UPN**> in format-list.
- How many times login failed for this user in last 30 days and tell me the reasons.
- Generate a report based on Entra plug-in: Is the user <**UPN**> considered risky? If yes, list the reasons.
- Show me the most recent failed sign-in for my account in the last month.
- What authentication methods are enabled for my account?
- List the groups I am part of
- List the groups <**Username**> is part of

Intune

- Which devices are used by user **<UPN>**
- Tell me about this device.
- Identify Weak hosts.
- Could you give me the total number devices in Intune?
- Show me configuration policies for this device.
- What groups is this device a member of?
- Tell me about managed apps on this device.
- Tell me about devices for <**Username**>
- show me the devices for **<username>**
- Show me the difference in managed applications for the above devices.
- How are managed apps on this device different from Shobhit's device? **(Shobhit is another user in this example)**
- What groups is <**Appname**> assigned to?
- Show me the users **<Notepad++ >**assigned to
- Show me the difference in the hardware for the above device
- Give me the status of the **<Devicename>**. Is it managed, is it compliant with management policies?
- Tell me about the app policy that isn't compliant. Why would this device be failing this policy?
- Tell me about the app policy that isn't compliant. Why would this device not have the policy applied and why is it in a state of non-compliance?

Defender & Sentinel

- Provide me a summary of Defender incident **<Incident ID>**
- Tell me more about Sentinel incident **<Incident ID>**
- Extract the entities associated with the incident.
- If a user is listed in the incident details, show which devices they have used recently and indicate whether they are compliant with policies.
- Are there any defender incidents involving **<Username>** on December 31st, 2023? List the title, severity, timestamp, Attack Techniques, and Categories for any incidents containing his account name or alias. Search account name containing **<User full name>** or **<user first name>**
- List the 10 most critical defender incidents.
- Write a PowerShell script to test the SMB versions and state across all the affected devices via remote connection.
- Write a PowerShell script to test the SMB versions and state across all the affected machines.
- Extract the entities from the script analysis **(If script analysis is done)**
- Write a report summarizing the investigation. Lead with a non-technical executive summary. Next provide the breakdown of the Defender incident report, the takeaways from the Sentinel Hunt, the Intune device state, and finally the threat intel summary
- Write a report summarizing the investigation. Lead with a non-technical executive summary. Next provide the breakdown of the Defender incident report, the takeaways from the Sentinel Hunt, the Intune device state, the threat intel summary, and finally next steps for remediation
- What are the critical Sentinel incidents right now?
- What are the critical Defender incidents right now?
- List the alerts on Sentinel incident **<Incident ID>**

- Check Defender for vulnerabilities related to **<CVE-XXXX>**
- List all Sentinel workspaces.
- List last 5 incidents from Sentinel workspace **<your-workspace>**
- Tell me more about **<Silk Typhoon>**, and include the IOCs and any TTPs associated with **<Silk Typhoon>?**
- show me MITRE TTPs from M365D incidents in the last month.
- What is the MITRE TTP number for account manipulation?

Threat Intelligence

- Summarize recent threat intelligence.
- What threat actors have been active lately?
- How should I harden my environment to prevent these attacks?
- Can you tell me about more specific threat intelligence related to the **<financial services industry>**?
- Can you help me with creating a KQL to search for relevant public IOCs from **<EvilProxy>** Phishing Attacks in Microsoft Defender? I would like to be able to search from a list of domains, IP addresses, and file hashes and add searching from alert evidence as well?
- Can you explain line by line what this KQL above is doing?
- Can you create the same KQL but adapt it for Sentinel?
- Write a KQL query to identity Log4J in my M365Defender and list resources that are impacted with Log4J vulnerability.
- It was observed that **<Manatee Tempest>** was active in this event. Provide a summary of the actor and their intersection with ransomware. ***Note: Replace threat actor name***
- Get me a profile of this threat actor **<Manatee Tempest>**
- Are there known TTPs for this threat actor?
- If there are TI articles related to this threat actor, provide a list and summary of them & include links in the last week.
- If there were TI articles found, what recommendations does the first article in the list have for protecting against this actor?
- Provide a summary of **<Mustard Tempest>** and a list of their brokered access methodologies.
- Summarize threat intelligence articles for **<"T1585.001">**
- Show me 5 indicators per actor for the actors above
- Show threat intelligence info for **<Aqua Blizzard>**
- Show relevant TTPs.
- Show relevant list of indicators.

Vulnerabilities

- Summarize the latest Vulnerabilities from the last week.
- Summarize **<CVE-XXXX>** vulnerability.
- What vulnerabilities have been exploited recently by threat actors?
- Which of these CVEs have known exploitations?
- Which technologies are impacted by each of these CVEs?
- Does **[CveId]** have known exploitations?
- Is my environment vulnerable to CVE **[CVEID]**?

Purview

- Show me the top 5 DLP alerts that I should prioritize today?
- Can you summarize purview alert **<AlertID>**?
- Can you summarize risk associated with user: **<UPN>** involved in this alert?
- What information does Purview have about the risk associated with this user?
- Which Purview Data Loss Prevention alerts should I prioritize today?
- Can you summarize the first purview alert?
- tell me more about the user <UPN>
- What was the data or action that triggered this alert?
- What are the data risks related to this alert?
- For the files related to the alert, show me all activities done in last 7 days?
- Can you get me the status of labelling on these files?
- What Suspicious Actions Have Been Performed on This Files?
- List all active Purview Policies covering the sensitive data in the file.
- What other DLP alerts are present for this user?
- According to Purview, what is the implication of these DLP Alerts?
- How many DLP policies have adaptive protection configured?

EASM

- Show me the attack surface summary for **<Woodgrove Bank>**
- How many domains are expired in the **<Woodgrove Bank>** organization's attack surface?
- How many SSL certificates are expired in the **<Woodgrove Bank>** attack surface?
- Are there any vulnerabilities impacting the host **<testsd.woodgrovebank.com>**?
- Provide the CVSS scores for the CVE IDs on the asset **<testsd.woodgrovebank.com>**
- What are the mitigation steps for the CVE **<CVE-ID>**?
- Show me the intel profile for **<Hazel Sandstorm>**
- Show me any associated indicators for the above actor.
- What are some of the domain indicators for this actor.
- Get me the reputations for hostname "service-logins.com"
- What are some of the web components for the ip address mentioned above?
- Get the most recent whois record for <manniewith98.com>
- Summarize threat intelligence articles related to the actor mentioned above.
- Are there any threat intelligence articles that reference the IOCs that were found?
- Show me the profiles of any threat actors referenced.
- Are any of these CVEs impacting my internet-facing assets?
- Is my environment vulnerable to any of the CVEs from the list above?
- Is my environment vulnerable to **CVE [CVEID]**?
- Check my cloud assets for vulnerabilities related to **<CVE-XXXX>**
- Create a report for this copilot session and include sections for: An Overview of MDEASM, The Summary of the Attack Surface for **<Woodgrove Bank>**, List of Expired Domains and whois info, The list of Common Names from Expired SSL Certificates, Describe the Vulnerabilities on the Host **<testsd.woodgrovebank.com>** with CVSS scores, Detailed Steps for Mitigating Vulnerabilities on **<testsd.woodgrovebank.com>**

Please review below-mentioned articles for your reference:

Microsoft Security Copilot
https://learn.microsoft.com/en-us/security-copilot/

API plugins in Microsoft Security Copilot
https://learn.microsoft.com/en-us/security-copilot/plugin_api

GPT plugins in Microsoft Security Copilot
https://learn.microsoft.com/en-us/security-copilot/plugin_gpt

KQL plugins in Microsoft Security Copilot
https://learn.microsoft.com/en-us/security-copilot/plugin_kql

Manage plugins in Microsoft Security Copilot
https://learn.microsoft.com/en-us/security-copilot/manage-plugins?tabs=securitycopilotplugin

Logic Apps connectors in Microsoft Security Copilot
https://learn.microsoft.com/en-us/security-copilot/connector_logicapp

The Microsoft Security Copilot Partner Private Preview
https://securitypartners.transform.microsoft.com/copilot-private-preview-partners