Microsoft Security

Prompt Engineering Best Practices

Get the most out of Microsoft Copilot for Security

What is Prompt Engineering?

The process of writing, refining, and optimizing inputs—or "prompts"—to encourage generative artificial intelligence (AI) systems to create specific, high-quality outputs is called **prompt engineering**. It helps generative AI models organize better responses to a wide range of queries—from the simple to the highly technical. The basic rule is that good prompts equal good results.

Prompt engineering is a way to "program" generative AI models in natural language, without requiring coding experience or deep knowledge of datasets, statistics, and modeling techniques. Prompt engineers play a pivotal role in crafting queries that help generative AI models learn not just the language, but also the nuance and intent behind the query. A high-quality, thorough, and knowledgeable prompt, in turn, influences the quality of AI-generated content, whether it's images, code, data summaries or text.

Prompt engineering is important because it allows AI models to produce more accurate and relevant outputs. By creating precise and comprehensive prompts, an AI model is better able to synthesize the task it is performing and generate responses that are more useful to humans.

The benefits of prompt engineering include:

It can improve the speed and efficiency of generative AI tasks, such as writing complex queries, summarizing data, and generating content.

It can enhance the skills and confidence of generative AI users especially novices by providing guidance and feedback in natural language.

It can leverage the power of foundation models, which are large language models built on transformer architecture and packed with information, to produce optimal outputs with few revisions.

It can help mitigate biases, confusion, and errors in generative AI outputs by fine tuning effective prompts.

It can help bridge the gap between raw queries and meaningful AI generated responses and reduce the need for manual review and post generation editing.

The following examples demonstrate the importance of clarity, specificity, and context in crafting effective prompts for generative AI.

Why good prompts are important

Prompt engineering is a skill that can be learned and improved over time, by experimenting with different prompts and observing the results. There are also tools and resources that can help people with prompt engineering, such as prompt libraries, prompt generators, or prompt evaluators.

How to use prompts in security

Prompting is very important in Copilot, as it is the main way to query the generative AI system and get the desired outputs. Prompting is the process of writing, refining, and optimizing inputs—or "prompts"—to encourage Copilot for Security to create specific, high-quality outputs.

Effective prompts give Copilot for Security adequate and useful parameters to generate valuable responses.

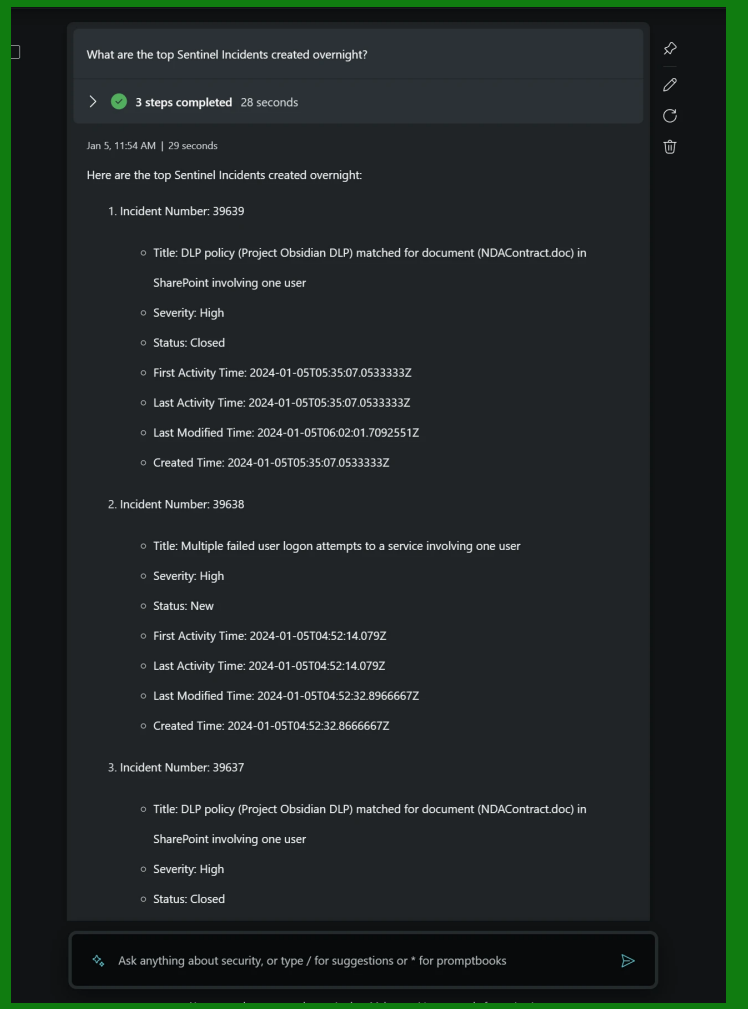
Security analysts or researchers should include the following elements when writing a prompt:

Goal - specific, security-related information that you need.

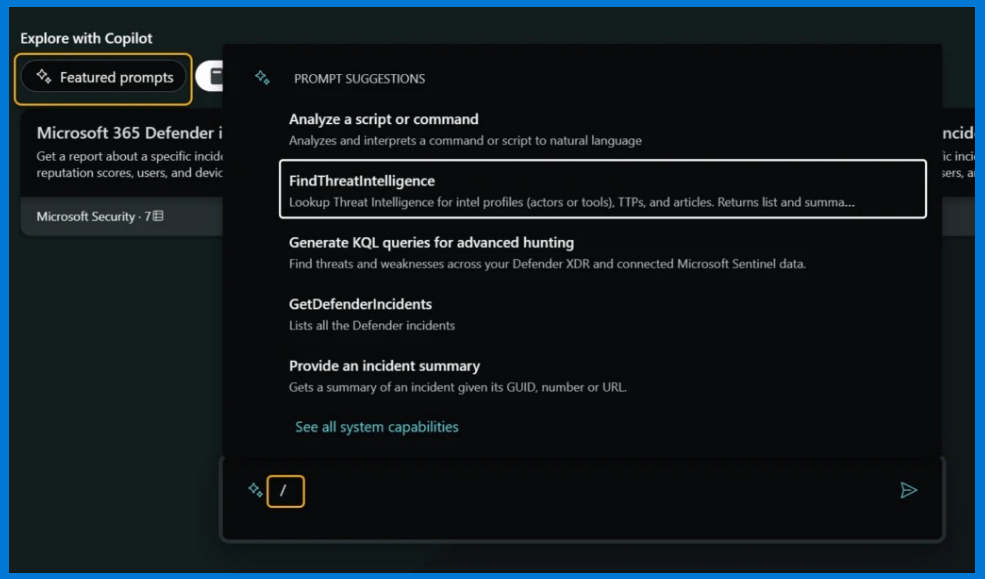
Context - why you need this information or how you'll use it.

Expectations - format or target audience you want the response tailored to.

Source - known information, data source(s), or plugins Copilot for Security should use.



By creating precise and comprehensive prompts, Copilot for Security can better understand the task it is performing and generate responses that are more useful to humans. Prompting also helps mitigate biases, confusion, and errors in Copilot for Security outputs by fine tuning effective prompts.



Featured prompts in Copilot:

Analyze script or command

Summarize security article

Generate security query

Generate security report

Save time with top prompts

Featured prompts are a set of predefined prompts that are designed to help you accomplish common security-related tasks with Copilot for Security. They are based on best practices and feedback from security experts and customers.

You can also access the featured prompts by typing a forward slash (/) in the prompt bar and selecting the one that matches your objective. For example, you can use the featured prompt "Analyze a script or command" to get information on a suspicious script or command.

Some of the featured prompts available in Copilot for Security are:

Analyze a script or command: This prompt helps you analyze and interpret a command or script. It identifies the script language, the purpose of the script, the potential risks, and the recommended actions.

Summarize a security article: This prompt helps you summarize a security article or blog post. It extracts the main points, the key takeaways, and the implications for your organization.

Generate a security query: This prompt helps you generate a security query for a specific data source, such as Microsoft Sentinel, Microsoft 365 Defender, or Azure Monitor. It converts your natural language request into a query language, such as Kusto Query Language (KQL) or Microsoft Graph API.

Generate a security report: This prompt helps you generate a security report for a specific audience, such as executives, managers, or analysts. It uses the information from your previous prompts and responses to create a concise and informative report.

Use promptbooks to save time

A promptbook is a collection of prompts that have been put together to accomplish a specific security-related task—such as incident investigation, threat actor profile, suspicious script analysis, or vulnerability impact assessment. You can use the existing prompt books as templates or examples and modify them to suit your needs.

Some of the promptbooks available in Copilot for Security are:

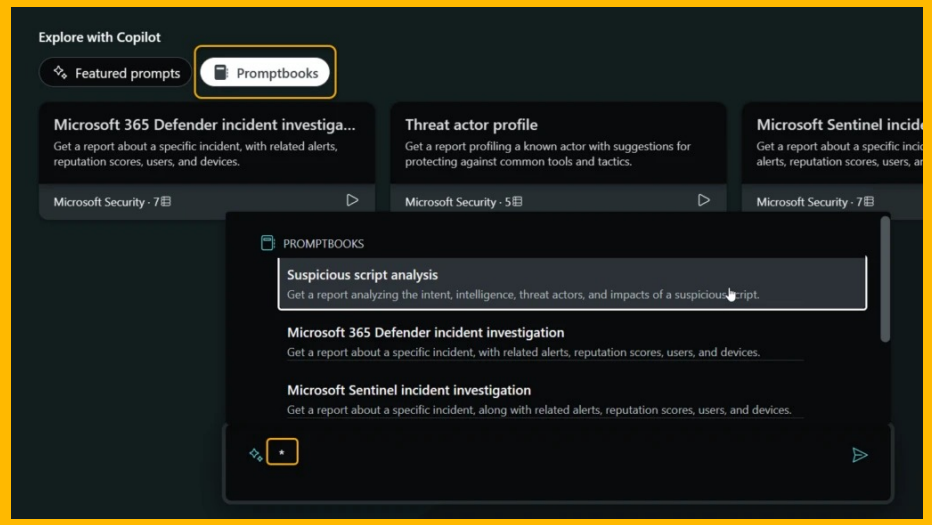
Incident investigation: This promptbook helps you investigate an incident by using either the Microsoft Sentinel or Microsoft 365 Defender plugin. It generates an executive report for a nontechnical audience that summarizes the investigation.

Threat actor profile: This promptbook helps you get an executive summary about a specific threat actor. It searches for any existing threat intelligence articles about the actor, including known tools, tactics, and procedures (TTPs) and indicators, and provides remediation suggestions.

Suspicious script analysis: This promptbook helps you analyze and interpret a command or script. It identifies the script language, the purpose of the script, the potential risks, and the recommended actions.

Vulnerability impact assessment: This promptbook helps you assess the impact of a publicly disclosed vulnerability on your organization. It provides information on the vulnerability, the affected products, the exploitation status, and the mitigation steps.

Using promptbooks in Copilot is a way to accomplish specific security-related tasks with a series of prompts that run in sequence. Each prompt book requires a specific input—such as an incident number, a threat actor name, or a script string—and then generates a response based on the input and the previous prompts. For example, the incident investigation prompt book can help you summarize an incident, assess its impact, and provide remediation steps.



To use a promptbook, you can either type an asterisk (*) in the prompt bar and select the promptbook you want to use or select the Promptbooks button above the prompt area. Then, you can provide the required input and wait for Copilot for Security to generate the response. You can also ask follow-up questions or provide feedback in the same session.

Common Copilot Prompts

The following list of prompts are an excerpt of the Top 10 prompts infographic, which provides prompts utilized and recommended by customers and partners with great success. Use them to spark ideas for creating your own prompts.

Get started with prompts from Copilot

We know creating precise and comprehensive prompts produces accurate, relevant responses. By understanding the fundamentals of good prompt engineering, security analysts can improve the speed and efficiency of generative AI tasks, mitigate biases, reduce output errors, and more—all without requiring coding experience or deep knowledge of datasets, statistics, and modeling techniques. The prompt engineering best practices described here, along with featured prompts and promptbooks included in Copilot for Security, can help security teams utilize the power of generative AI to improve their workflow, focus on higher-level tasks, and minimize tedious work.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (@MSFTSecurity) for the latest news and updates on cybersecurity.

Learn more about Microsoft Copilot for Security
https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot

Read the full Top 10 Prompts infographic
https://go.microsoft.com/fwlink/?linkid=2259753&clcid=0x409&culture=en-us&country=us