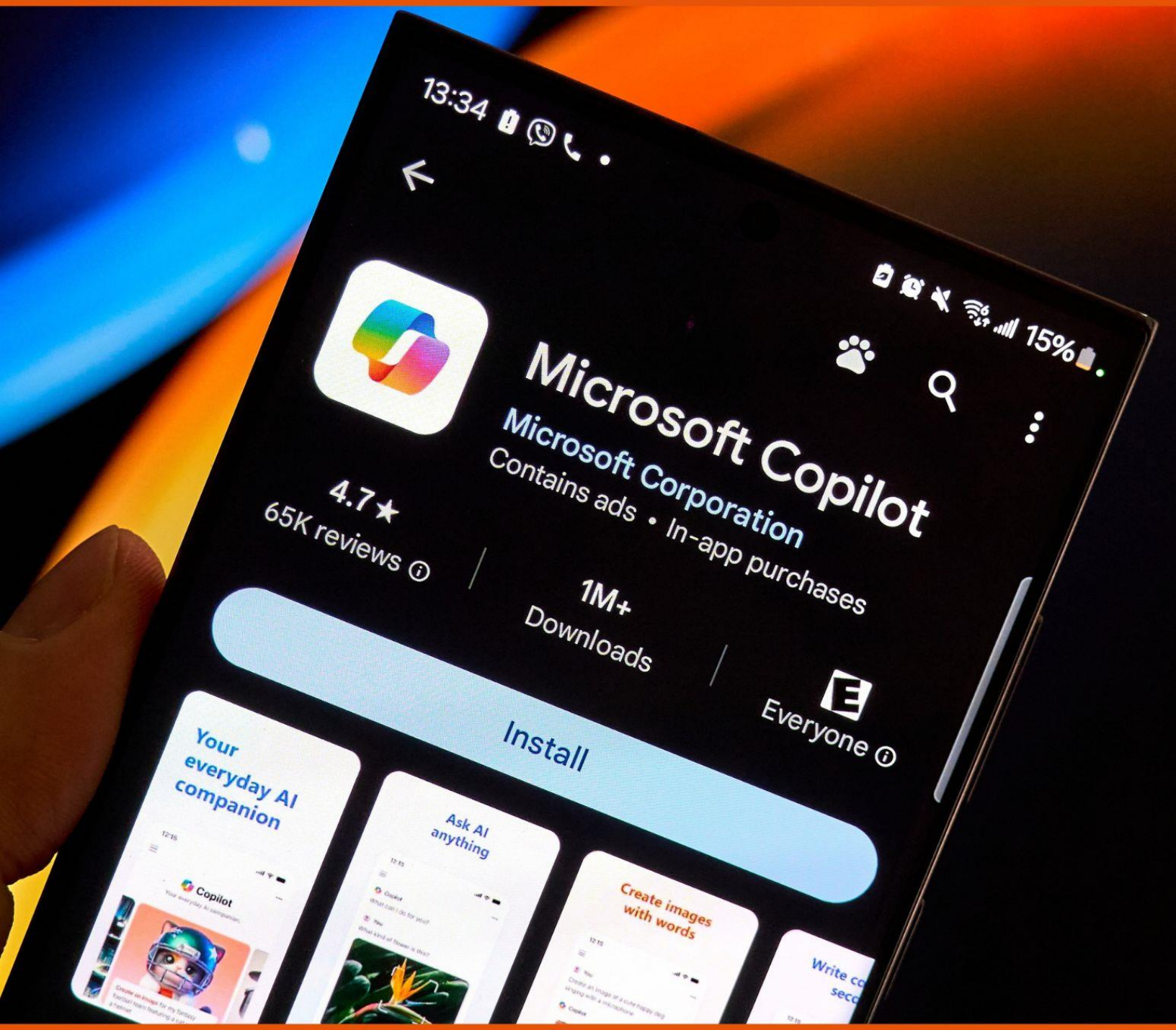
An Introduction Microsoft CoPilot For Security

A Whitepaper Written For KAMIND IT, Inc.



By Ravi Das

Contents

Introduction

In all of the world in Cybersecurity, the biggest buzzword of all time is that of Artificial Intelligence, also known more commonly as just "AI". This is actually a very wide field, and although it has just recently caught a lot of fire, it actually has been around for quite a long time, even going back all the way to the 1940s. Many models, algorithms, and applications have been developed since then. Probably the most notable application that has evolved so far has been that of ChatGPT.

Although this was developed and launched primarily by the firm known as OpenAI, Microsoft also had a huge role in its evolution. For example, it is primarily hosted on Azure, and through its alliance with OpenAI, Microsoft has been able to produce a new offering known as "Azure OpenAI". It is a SaaS based deployment, and can be found in the Marketplace as you log into your Azure subscription.

What Is Artificial Intelligence?

But before we delve further into this whitepaper, it is first important to define what Artificial Intelligence is. A technical definition of it is as follows:

"Artificial intelligence, or AI, is technology that enables computers and machines to simulate human intelligence and problem-solving capabilities."

(SOURCE: https://www.ibm.com/topics/artificial-intelligence)

In other words, in any model or algorithm that is developed, the goal of AI in the end is to try to mimic as much as possible the thinking and reasoning processes of the human brain. While the research in this area will continue to grow and advance well into the future, it is important to keep in mind that we will never fully replicate or at the very least – even understand the human brain. At best, we may just grasp 0.5% and no more.

What Is Machine Learning?

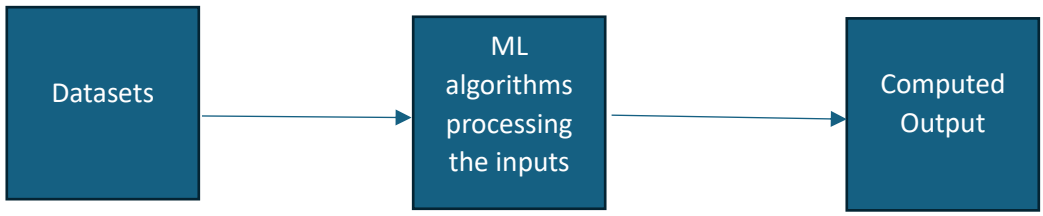
But within the realm of Artificial Intelligence, there are also other subfields that evolved from it as well. One of these is called "Machine Learning", also known as "ML" for short. A technical definition of Machine Learning is as follows:

"Machine learning (ML) is a type of artificial intelligence (AI) focused on building computer systems that learn from data."

(SOURCE: https://www.techtarget.com/searchenterpriseai/definition/machine-learning-ML).

The basic premise here is that once you have developed a specific model, then through the process of the Machine Learning algorithms, you can input (or "ingest") datasets into it, and from there, derive an output, in which most cases, will be an answer to a query.

An example of this is illustrated below:

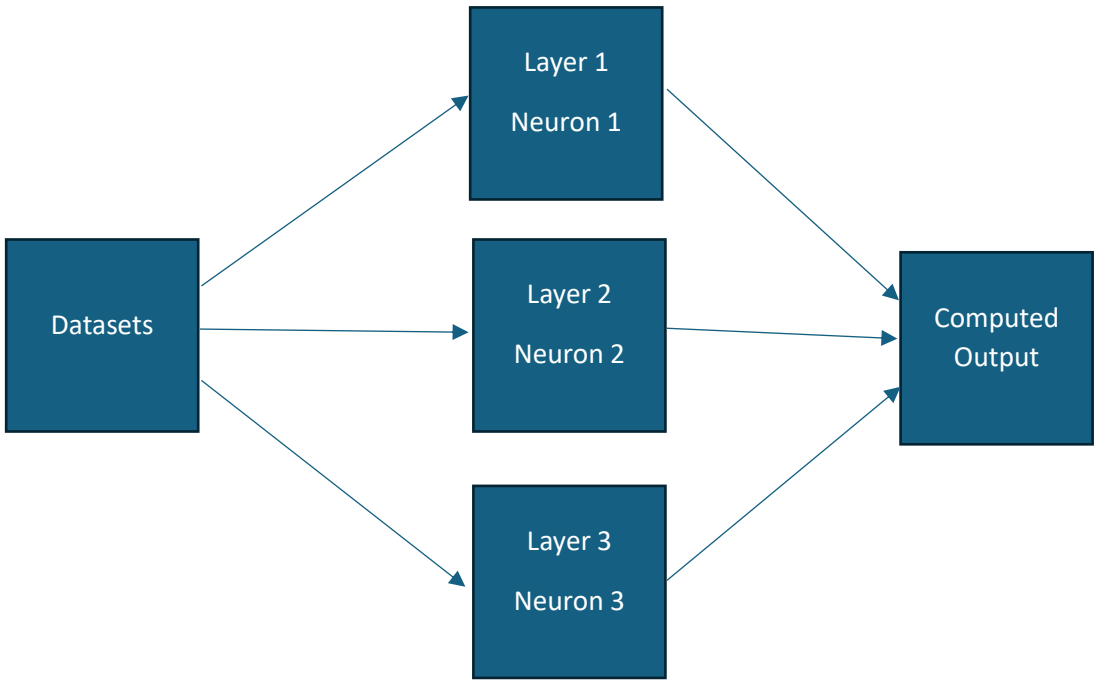


Another important aspect of AI is that of the Neural Network. It can be technically defined as follows:

"Machine learning teaches machines to learn from data and improve incrementally without being explicitly programmed."

(SOURCE: https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-ml/)

In fact, the Neural Network can be considered as a much more advanced version of Machine Learning. For example, it makes of mathematical representations of the main cell in the human brain, which is known as the "Neuron". These Neurons, then in turn, are deployed to within the different layers in the Neural Network algorithms. An illustration of this is seen below:



What Is Natural Language Processing?

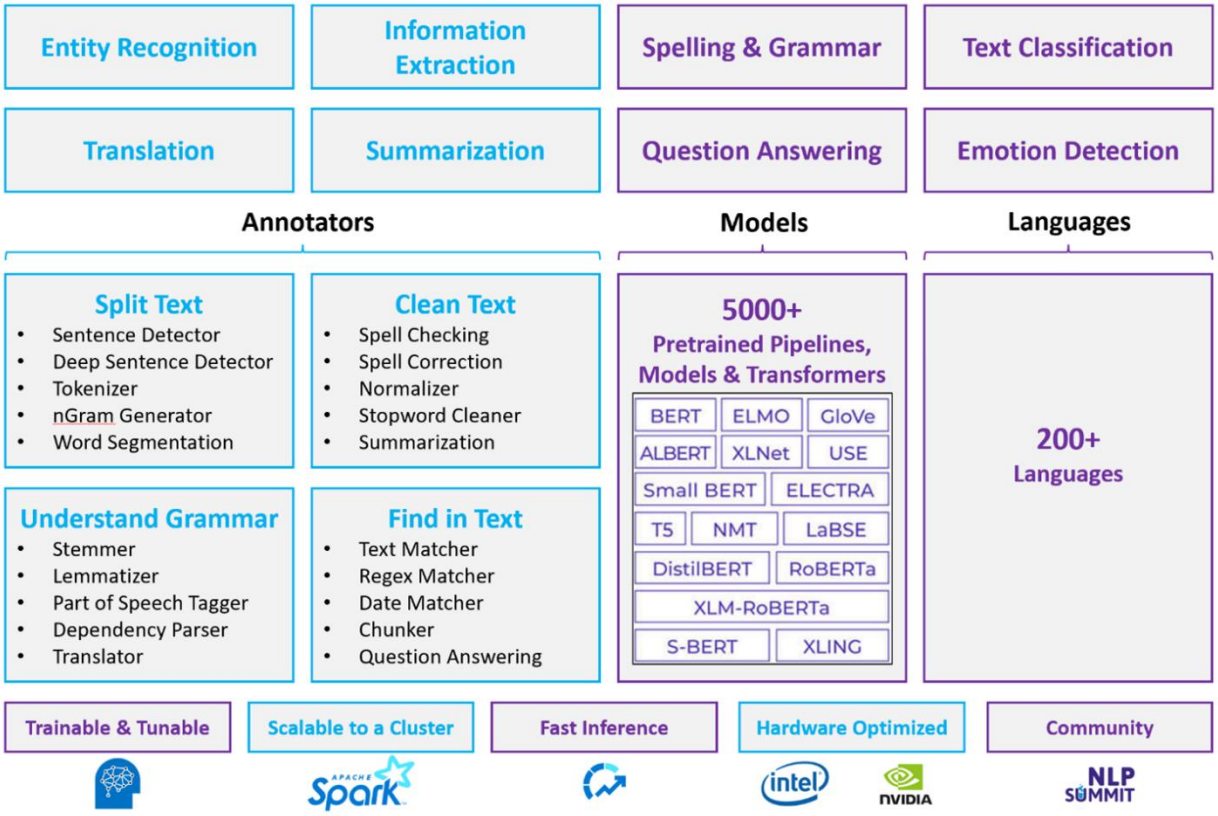
Finally, another area of AI that is starting to boom is that of “Natural Language Processing”, also known as “NLP” for short. A technical definition of it is as follows:

“Natural language processing (NLP) is a machine learning technology that gives computers the ability to interpret, manipulate, and comprehend human language.”

(SOURCE: https://aws.amazon.com/what-is/nlp/).

In other words,

Simply put, the AI algorithms attempts to replicate human language (either in written or spoken form) as the output. An example of Natural Language Processing is below, as it also appears in Azure:



(SOURCE: https://learn.microsoft.com/en-us/azure/architecture/data-guide/technology-choices/natural-language-processing)

It is the combination of Machine Learning, Neural Networks, and Natural Language Processing that forms the AI driven solution, or backbone of the latest release from Microsoft, which is the CoPilot For Security.

CoPilot For Security And Cybersecurity

As its name directly implies, Microsoft CoPilot has been designed primarily for the CISO and their corresponding IT Security teams. It can fit and be used by all kinds of businesses, from the smallest of the small to the largest of the large. It is meant to give you give the latest on the Cyber Threat Landscape, so that you can stay one ahead of the Cyberattacker. Here are some examples as to how it can help you in that regard:

1) A one stop shop for viewing:

   Many businesses of today are using many kinds of security tools and technologies from a plethora of different vendors. But in the end, using too many of them will only increase your attack surface, thus making it that much easier for the hacker to penetrate into. Therefore, the latest advice is to try to conduct a Risk Assessment as to where all of your security devices lie at, and from there, regroup them as to where they can be best used. By doing this, you will also shed some redundant tools and technologies as well. CoPilot For Security can help you map all of this one holistic view, so that not only you can document where everything is at, but even get a detailed visual on it so that you can map your new strategy accordingly. Also, it can take all of the information and data that is provided by your log files, and sift through all of them. From there, it can provide those pieces that are most relevant and important to your IT Security team, by filtering out all of the noise. That way, you can get a very quick view into any kind of abnormal activity (such as an unusual amount of logins), and even ask CoPilot For Security for recommendations on what to do. This is where the Generative AI component comes into play. In fact in some ways, this can be a total replacement for your SIEM software package/

2) A decrease:

   The average time it takes for an average sized business to actually detect and respond to a threat variant is now pegged at seven months. This is reflected in the "Mean Time To Detect" ("MTTR") and the "Mean Time To Respond" ("MTTR") metrics. Given the deep level of sophistication that CoPilot For Security clearly demonstrates, it is highly expected that this large time gap will eventually, over time, be brought to just a matter of a few hours. As a result***, the cost it takes to subscribe to this platform is just a fraction of what a security breach will really cost you in the end.***

3) Training:

   One of the reasons why there is such a huge shortage in the Cybersecurity Workforce today is that hiring managers are very reluctant to have to train people who are college or trade school graduates with little experience. But CoPilot For Security can help alleviate this to a large extent, by actually providing actual training for new hires, by indoctrinating them into the details of your IT and Network Infrastructure, as well as your Security Polices. Thus, this will free up time for

the senior members of your IT Security staff to focus on fending off the inbound threat variants that are aimed at your business.

4) Get quick answers:

By using the power of Generative AI, you can ask CoPilot For Security just about anything Cyber related, and it will give the most appropriate response. Here are some examples of this:

- Security Operations:

  If you have a question about how to resolve an issue, you can directly speak into it (via the powers of Natural Language Processing) and it will produce the right answers that you need in just a matter of seconds. More details can be downloaded at the link below:

  http://cyberresources.solutions/CoPilot_Security_WP/CoPilot_SOC_WP.pdf

- Device Management:

  You can ask it the status of any device, and with the advancements made in Geo Location, it will track it down and give you all of the information that you need about it.

- IAM:

  This is an acronym that stands for "Identity and Access Management". Through this methodology, you assign the rights, privileges, and permissions for all of your employees to gain access to not only their own devices, but to shared resources as well. You can use CoPilot For Security to keep a continuous watch on all of your user profiles and accounts, in an effort to make sure that you are following the concepts of "Least Privilege". It will come in also very useful for monitoring Privileged Access Accounts (this is where you assign super user level rights, permissions, and privileges), which is a top prize for the Cyberattacker to go after.

- Data Management:

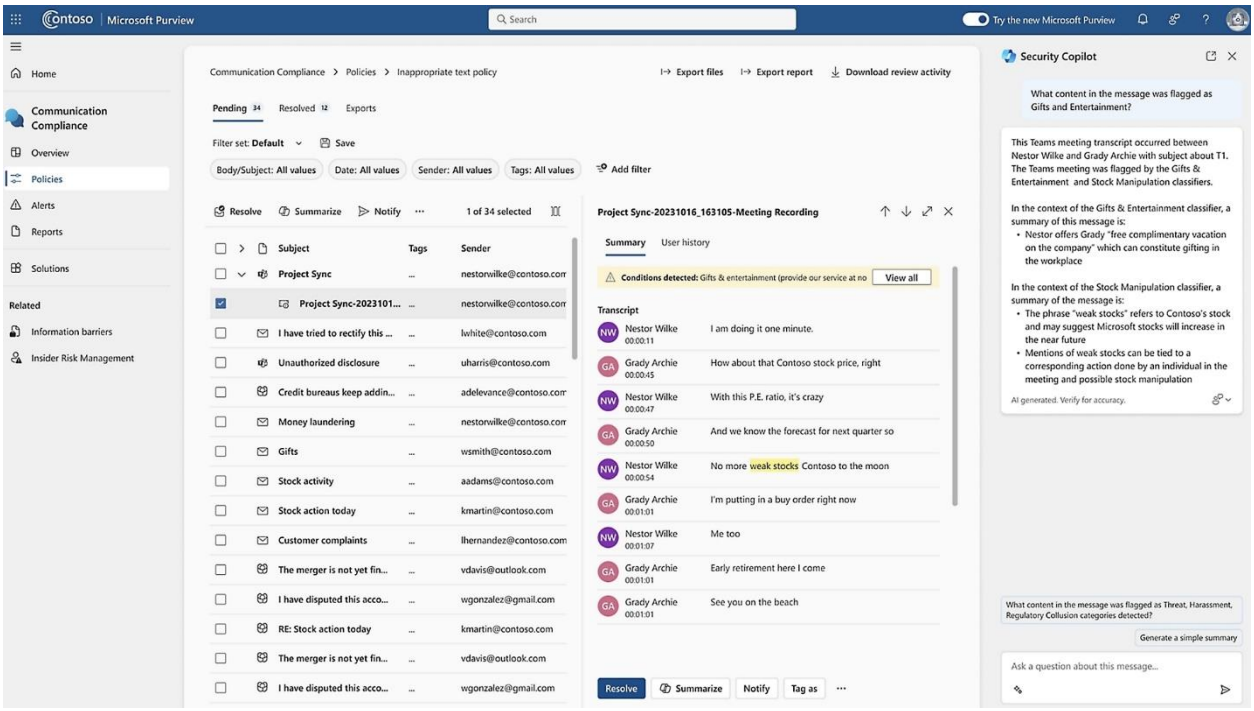
  When it comes to this, this is a huge area in which CoPilot For Security can help you with. Here are some examples:

  *Making sure that you are coming into compliance with the data privacy laws such as the GDPR, CMMC, HIPAA, CCPA, etc.

  *Making sure that the controls that you have in place are optimized in order to mitigate the risks of data loss and exfiltration.

  *Calculating a risk profile for each employee (based on past network activity) to determine who could be a potential risk to your IT and Network Infrastructure.

  *You can get a holistic of all of the above, through one console, which is illustrated below:



(SOURCE: 1).

- A quick process:
  CoPilot For Security follows a very simple, five step process to answer all of your queries and action items. They are as follows:

  *Ascertains the initial context of the query (this is the "Orchestrator" component).

  *Creates a plan for the output (this is the "Build Context" component).

  *Analyzes all data to find any hidden trends (this is the "Plugins" component).

  *Combines all of the data and context of the query to formulate the output (this is the "Responding" component).

  *Output is computed (this is the "Response" component).

This is all illustrated below:

(SOURCE: 1).

The Use Of Custom Promptbooks

Since a major component of CoPilot For Security is Generative AI, it is important to review what exactly "Prompt Engineering" is all about. First, let us start out with a simple example of doing a Google search. You enter certain keywords, a statement, or even a direct question. Within seconds, entire web pages of resources that you use to find the answer appears. The key here is that you actually had to enter something in order to get a response.

The same also holds true for all versions of CoPilot that have been released, even this one. But since it is powered by so many powerful kinds of Generative AI algorithms, it can pull through far more many resources than what a traditional Google search can do. Further, it does not give you a selection of resources to look through to find you answer, rather, it gives you the answer directly (which is also the "Output"). So in order to get the best possible answer to your query, you have to be very precise in the kinds of keywords that you put into your query. The art of doing this is called "Prompt Engineering", and it can be technically defined as follows:

"Prompt engineering is the practice of designing and refining prompts—questions or instructions—to elicit specific responses from AI models."

(SOURCE: 2).

So, the bottom line here is that the more refined and specific of a query you can give, the better the response, or the Output will be. However, there is no silver bullet to mastering Prompt Engineering, it

simply takes a lot of trial and error. But Microsoft has introduced a new concept in the CoPilot For Security called the "Promptbook". They have defined as follows:

"Promptbooks [are] a collection of prompts that have been put together to accomplish specific security-related tasks. Each promptbook requires a specific input (for example, a code snippet or a threat actor name)."

(SOURCE: 3).

In other words, it is a repository of saved prompts that you can use directly, or even further customize to fit your security requirements. You can also save them here for further reference, as well. The next few subsections provide examples in how to do this.

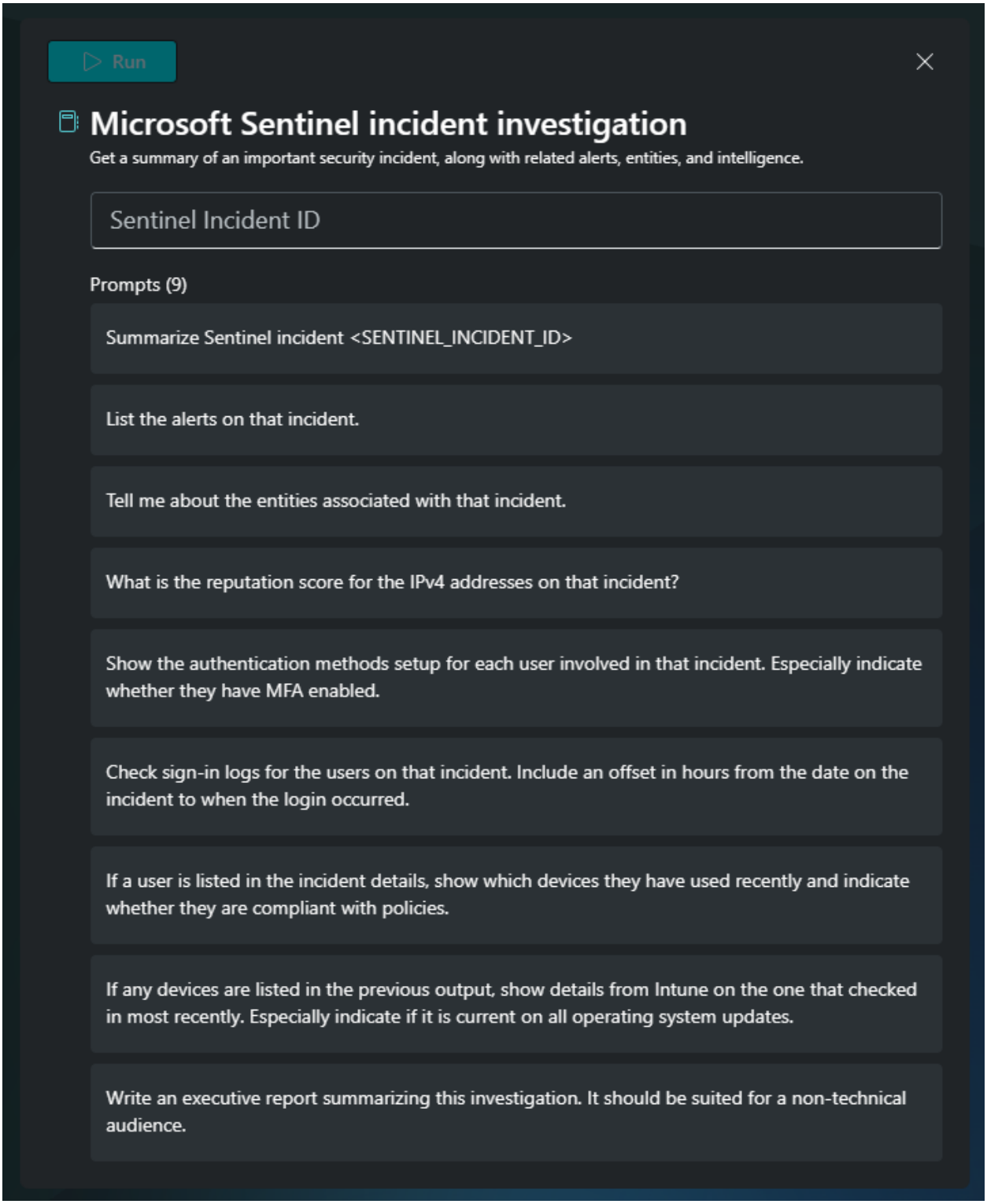
For Incident Response

For this scenario, follow these steps:

1) Launch Microsoft Sentinel/

2) Enter an asterisk (*) at the Prompt Bar.

3) Select "Microsoft Sentinel Incident Investigation." This is illustrated in the diagram below:



(SOURCE: 3).

4) Select an Incident Identification Number.

5) Select “Run”.

6) Wait for CoPilot For Security to process your request.

7) Once it is done, it will display a set of recommendations for you to follow to resolve this particular incident.

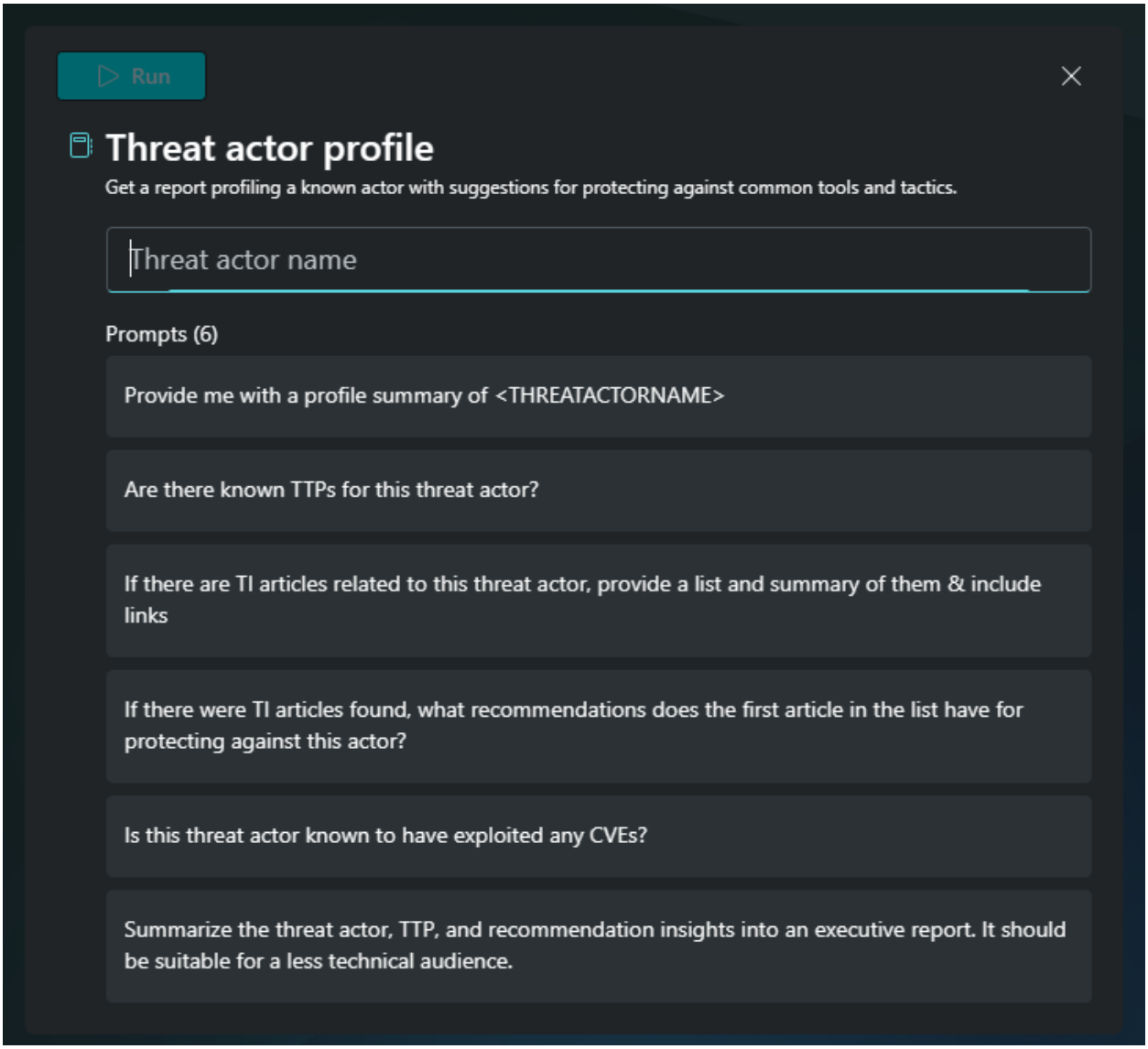
For A Threat Actor Profile

For this scenario, follow these steps:

1) Launch Microsoft Sentinel.

2) Enter an asterisk (*) at the Prompt Bar.

3) Select “Threat Actor Profile.” Enter the name of the Threat Actor., where is says “Threat Actor Name”. This is illustrated in the diagram below:



(SOURCE: 3).

4) Select “Run”.

5) Wait for CoPilot For Security to process your request.

6) Once it is done, it will display a set of recommendations for you to follow to identify and get more details about this particular Threat Actor.

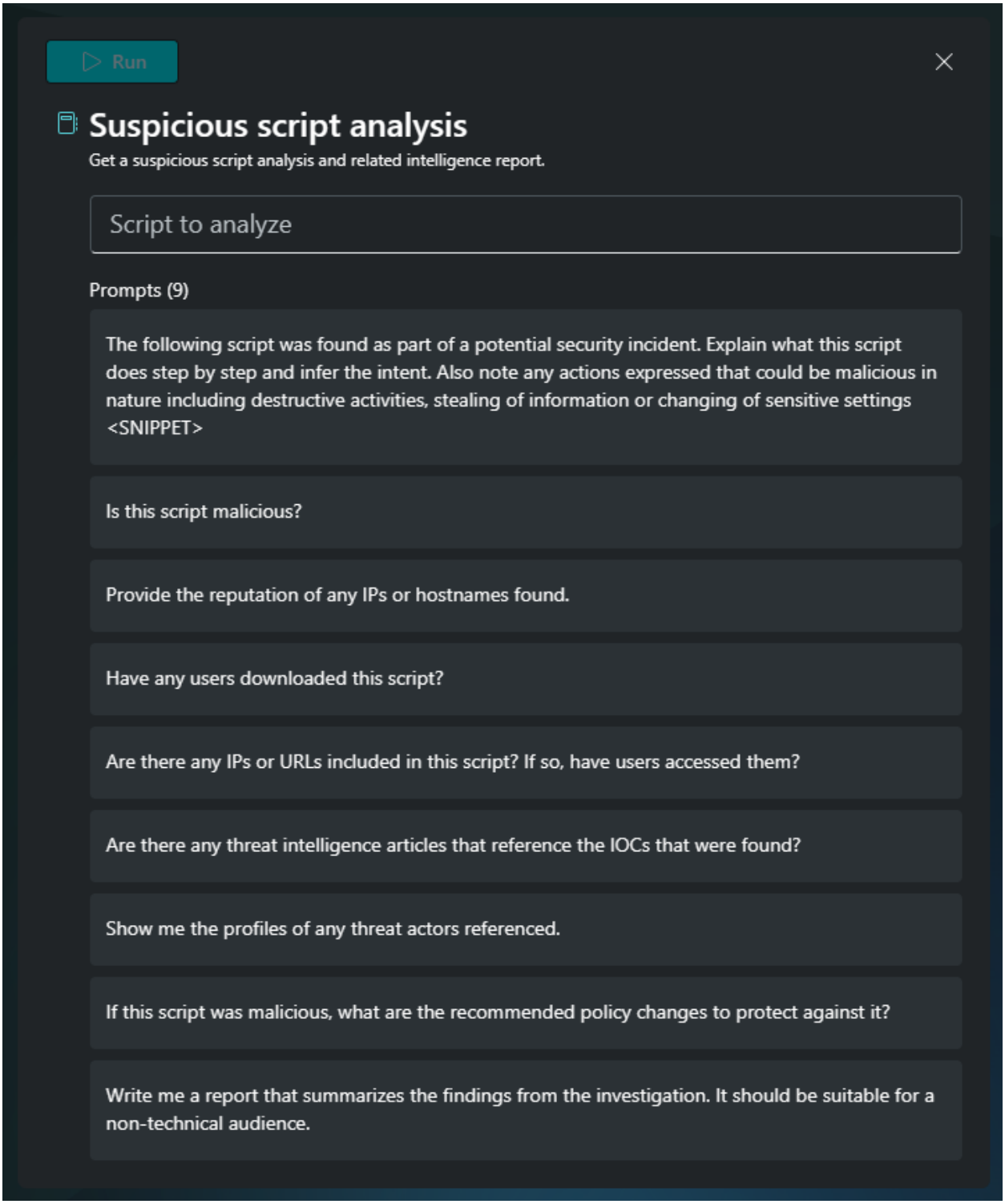
For Suspicious Script Analysis

For this scenario, follow these steps:

1) Launch Microsoft Sentinel.

2) Enter an asterisk (*) at the Prompt Bar.

3) Select “Suspicious Script Analysis.” Copy and paste your selected script where it says, “Script To Analyze”. This is illustrated in the diagram below:



(SOURCE: 3).

4) Select “Run”.

5) Wait for CoPilot For Security to process your request.

6) Once it is done, it will display a set of recommendations for you to follow to identify and get more details about the vulnerabilities and courses of remediation in your script.

   NOTE: This tool is primarily designed for analyzing PowerShell Scripts.

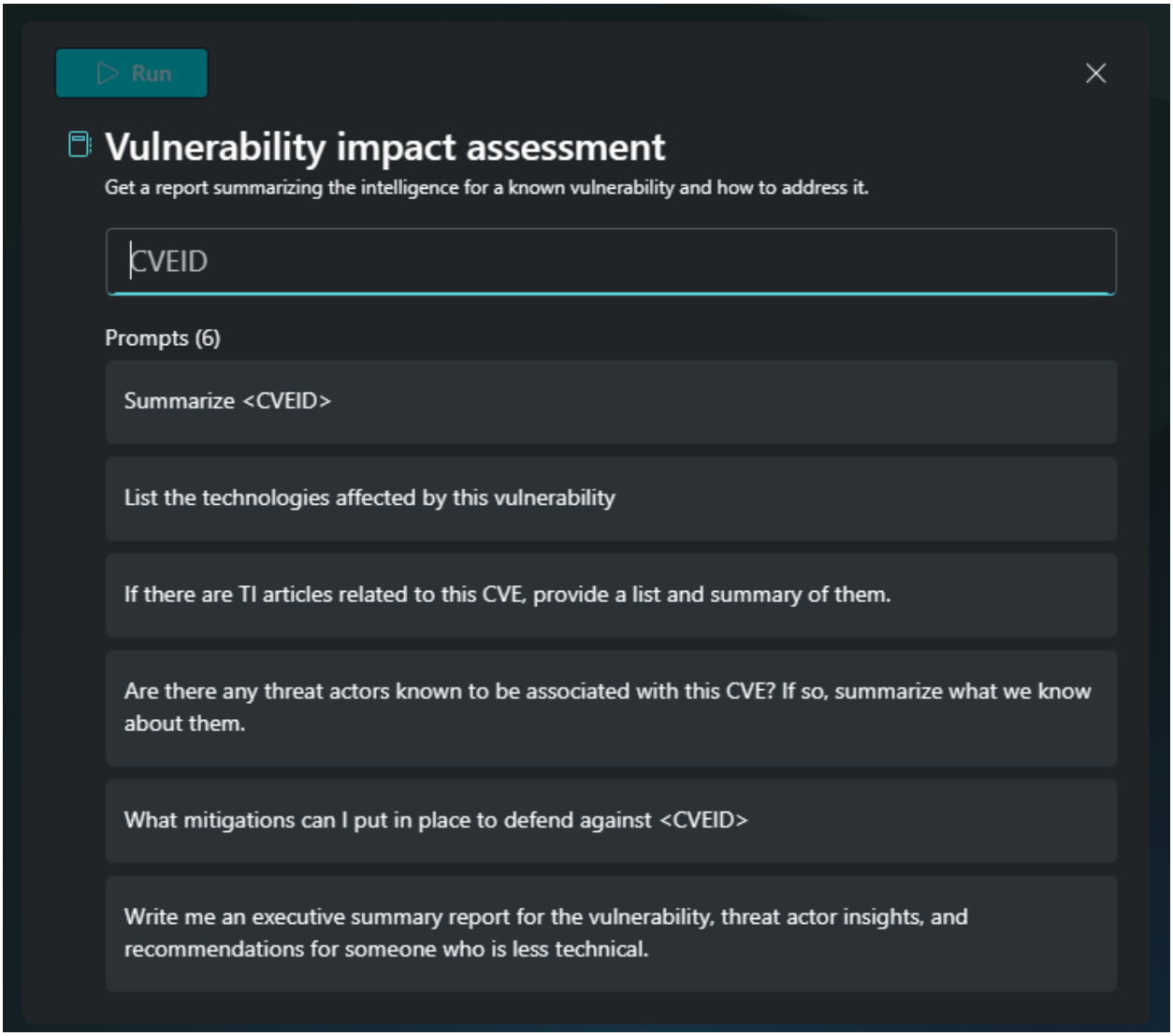
For The Vulnerability Impact Assessment

For this scenario, follow these steps:

1) Launch Microsoft Sentinel.

2) Enter an asterisk (*) at the Prompt Bar.

3) Select “Vulnerability Impact Assessment.” Enter the CVE number where it says “CVEID”. This is illustrated in the diagram below:



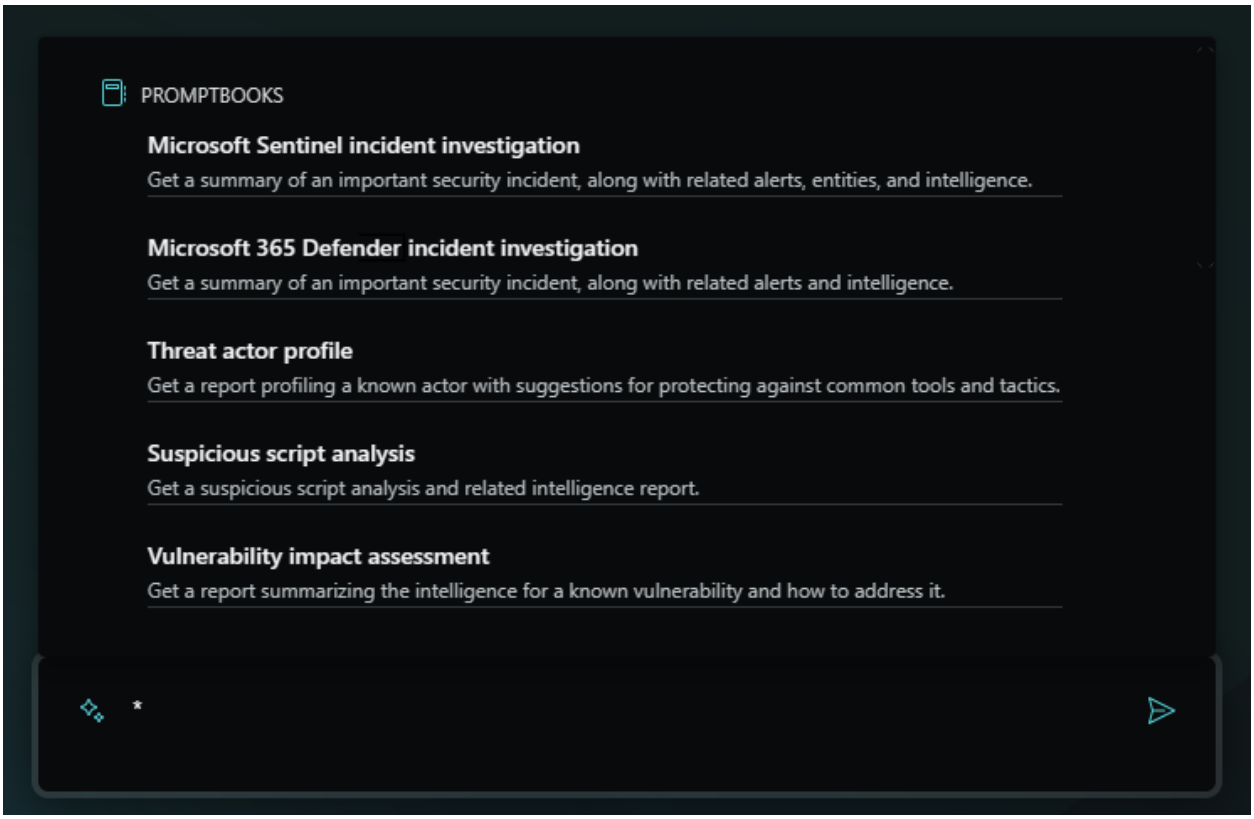
(SOURCE: 3).

4) Select “Run”.

5) Wait for CoPilot For Security to process your request.

6) Once it is done, it will display a set of recommendations for you to follow to identify and get more details about the exploitation possibilities and courses of remediation for you to follow in mitigating it.

The above reviewed features can also be seen from a single screen, which is illustrated below:



(SOURCE: 3).

To get more details onto to appropriately use Prompt Engineering in CoPilot For Security, click on the link below:

http://cyberresources.solutions/CoPilot_Security_WP/CoPilot_Security_Prompt_Engineering.pdf

Finally, the matrix below reviews guidelines in how to create effective prompts in CoPilot For Security:

Objective	*End Result*
The Goal	It should be specifically to your security concern.
The Context	Describe why you need this/how you will apply it.
The Expectation	The audience as to whom the Output will be targeted.
The Source	Cite any Data Sources, or install any needed Plug Ins.

Third Party Integrations For CoPilot

From within your M365 subscription, there are a number of products that will integrate with CoPilot For Security. They are as follows:

1) Your holistic approach point of view:

   It can integrate with Microsoft's "Unified Security Operations Platform". This combines Microsoft XDR and your SIEM software package into one bundle. More information about this can be seen at the links below:

   https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security?https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot&ef_id=_k_EAIaIQobChMIqevy34WShQMVAHNHAR3yqwZQEAAYASAAEgL5A_D_BwE_k_&OCID=AIDcmmdamuj0pc_SEM__k_EAIaIQobChMIqevy34WShQMVAHNHAR3yqwZQEAAYASAAEgL5A_D_BwE_k_&gad_source=1&gclid=EAIaIQobChMIqevy34WShQMVAHNHAR3yqwZQEAAYASAAEgL5A_D_BwE#modal-1234

2) Microsoft Intune:

   With this, you can do the following:

   - Reduce Cyberthreats to all of your devices, whether physical or virtual based.
   - Add extra layers of protection to your datasets.
   - Come into compliance with the GDPR, CCPA, HIPAA, etc. in your Azure Cloud Deployment.

   More information about this can be seen at the links below:

   https://www.microsoft.com/en-us/security/business/microsoft-Intune

3) Microsoft Purview:

   With CoPilot For Security embedded into this platform, you can create new strategies as to how your business can come into compliance with the data privacy laws. This is especially useful if after conducting an assessment, there are still some gaps that remain. More information about this can be seen at the link below:

   https://www.microsoft.com/en-us/security/business/microsoft-purview

4) Microsoft Sentinel:

   This is a platform that is available in your M365 subscription to collect data from all of your network security devices and correlate all of them together to present one, concrete picture of your Cyber Threat Landscape. More information about this can be seen at the link below:

https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-sentinel

5) Defender Threat Intelligence:

   This platform, coupled with CoPilot For Security, will allow you to collect intelligence and data on a real time basis. As a result, this allows for your Threat Hunting team to accurately gauge what could potentially happen in the Cyber Threat Landscape. More information about this can be seen at the link below:

   https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-threat-intelligence

6) Defender External Attack Surface:

   This tool from Microsoft allows you and your IT Security team to see threat variants on a real time map from the external environment. It can connect with the above-mentioned platforms to keep this map updated on a real time basis. More information about this can be seen at the link below:

   https://www.microsoft.com/en-us/security/business/cloud-security/microsoft-defender-external-attack-surface-management

7) XDR:

   In collaboration with CoPilot For Windows, this solution is geared primarily to protecting the endpoints in your IT and Network environment. These could be wireless devices, servers, workstations, and those that are in a virtual environment as well. More information about this can be seen at the link below:

   https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-xdr

8) Entra:

   This is a tool used to create and enforce Identity and Access Management (IAM) policies throughout not only your IT and Netwok Infrastructure, but also your entire business.

   https://www.microsoft.com/en-us/security/business/microsoft-entra

CoPilot For Security can also integrate with non-Microsoft products as well, in terms of other compatible Plugins that they offer. For a listing of them, click on the link below:

https://securitypartners.transform.microsoft.com/copilot-private-preview-partners?culture=en-us&country=us

Foreign Language Support

At the present time, CoPilot For Teams can support the following languages:

- Chinese (the simplified version)
- English
- French
- German
- Italian
- Japanese
- Brazilian Portuguese
- Spanish

It is important to note that there will be seventeen other foreign languages supported, but this will be supported through a different interface in CoPilot For Security.

Conclusions – Pricing

The pricing on CoPilot For Security is not quite as straightforward as it is for the other versions of CoPilot (which is just a monthly flat fee per user). While the good news is that it is based on a model of consumption usage (meaning you only pay for what you actually use), the actual cost is $4.00 SCU per hour. SCU is an acronym that stands for "Security Compute Unit". This is how it is defined per Microsoft:

"It is a unit of measurement of computing capacity to run a given workload."

(SOURCE: 4).

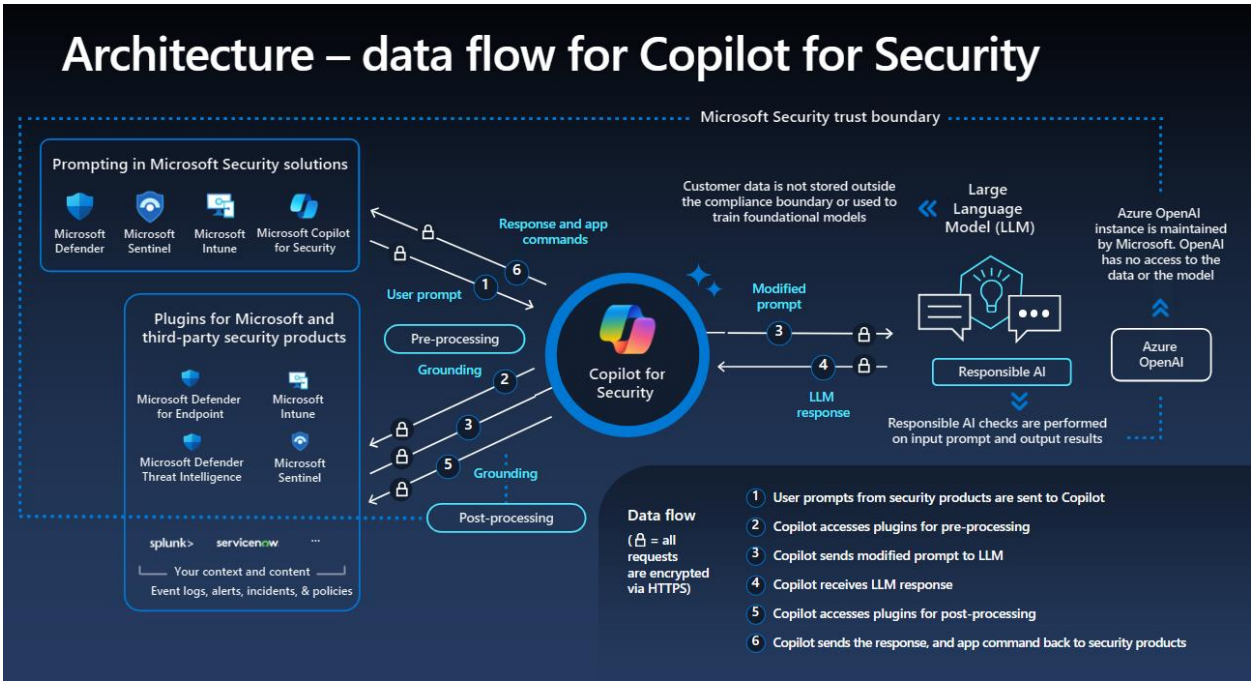
In this regard, 1 SCU is equal to 10 workflows per day. But, in order to start using CoPilot For Security, you must have at least one active SCU on a 24 X 7 X 365 basis. You purchase these SCUs in your Azure subscription, or from your Cloud Services Provider. But, you can scale up or down, as long as you still maintain that 1 SCU at all times.

We realize that this pricing model is probably confusing at first, but please contact us today if you need any help or have questions.

But for more guidance on how to manage your SCUs, click on the link below:

https://microsoft.github.io/PartnerResources/skilling/microsoft-security-academy/microsoft-security-copilot#:~:text=real%2Dtime%20visibility.-,Pricing%F0%9F%93%8C,SCU%20~10%20workflows%2Fday.

Finally, the illustration below reviews some of the major concepts that we have examined in this whitepaper:



Sources

1) https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-copilot-security#tabs-oc19f7_tab3
2) https://www.datacamp.com/blog/what-is-prompt-engineering-the-future-of-ai-communication
3) https://learn.microsoft.com/en-us/security-copilot/using-promptbooks
4) https://microsoft.github.io/PartnerResources/skilling/microsoft-security-academy/microsoft-security-copilot#:~:text=real%2Dtime%20visibility.-,Pricing%F0%9F%93%8C,SCU%20~10%20workflows%2Fday.