The Integration of Purview And CoPilot

A Whitepaper Written For KAMIND IT, Inc.

By Ravi Das

Table of Contents

A Review Of Microsoft CoPilot and Microsoft Purview

Introduction

As we all know, just in the last few years, Artificial Intelligence (AI), especially that of Generative AI, has been making a big splash. The primary driver for this has been ChatGPT, which was developed by OpenAI. Microsoft also played a big part in this, by leveraging a partnership with them, and also being the primary Cloud Provider for the platform. Because of this. Microsoft has developed many new Generative AI based tools for both Azure and M365.

Two of the most recent ones are those of CoPilot, and the Purview AI Hub. We will examine these in closer detail in this whitepaper, and how the two can be used together to help ascertain and mitigate your level of Cyber Risk.

What Is CoPilot?

Microsoft defines CoPilot as follows:

"It combines the power of large language models (LLMs) with your data in the Microsoft Graph—your calendar, emails, chats, documents, meetings, and more—and the Microsoft 365 apps to turn your words into the most powerful productivity tool on the planet."

(SOURCE: 1).

In other words, CoPilot is literally like your assistant – producing more innovative ways to create more powerful documentation, provide great data analysis, and creating compelling presentations. Here it is how it is being used the three main M365 tools:

1) Microsoft Word:

   It can help you with the entire compilation of the document that you are working on. It can not only produce new ideas of write to about, but it can also edit and proofread at the same time while you are writing. So, there is no need any more to hit the "Editor" button, and navigate through all of the changes it is recommending. You can pull in other content also from your other M365 products that you might be using. CoPilot will even suggest the kinds of tonalities that you should be using in your document. It can even provide recommendations as to how you can make any arguments or cases that you are presenting even stronger and more believable.

2) Microsoft Excel:

   This spreadsheet application has long been used by businesses in order to store and analyze data. But over time, it has become much more advanced, and to a novice user, it can become quite difficult to navigate through. But with CoPilot, all of this is taken away, and using Excel has never been any easier. All you have to do is merely ask a question, and CoPilot will find the answer in just a matter of a few seconds. Here are some examples:

- How can I create a macro?
- What hidden trends do you see in the data that is on the spreadsheet?
- Based upon the sales numbers already entered, can you predict how the next couple of quarters will look like?

CoPilot can even create new visualizations of the data and any projections by simply asking it. No need to waste time in trying to figure out what the X and Y axes should be. You can even ask it different "what if scenarios" and use that to provide solid recommendations to your higher ups.

3) Microsoft PowerPoint:

This has been the predominant tool used by businesses in order to create presentations. But just like Excel, this product has also become quite advanced, and it can take quite a bit of time to figure out how to create the best presentation possible. With CoPilot, all of these headaches are taken away from you. All you have to do is ask it to create a presentation based upon the data and content that you feed into, and minutes, you will have a compelling presentation to give in order to close that sales deal. Here are some of the other things that CoPilot can also do:

- Condense long presentations into shorter ones;
- Adjust layouts;
- Reformat content and other visuals;
- Fine tune the timing of animations.

The Other Applications Of CoPilot

Apart from the primary Office Product offerings in M365, CoPilot can also be used for the following subscriptions as well:

1) CoPilot In Teams:

When the COVID-19 pandemic hit, video conferencing became all of the rage. Now that it is more or less over, the one package that stands out from the rest of the crowd is that of Microsoft Teams. When CoPilot is used here, you can automatically launch meetings, have minutes taken, and even have the entire conversation recorded for future reference. CoPilot can also summarize the video conference call for you, and create a list of both follow and action items for the people on the call.

2) CoPilot In Loop:

This is a new software tool from Microsoft, and it is deemed to be one of the most sophisticated collaborative platforms out in the market today. CoPilot now kicks this up one more notch by creating the appropriate prompt queries, creating tables to help organize team projects, and even letting you take off where your teammates left off. In other words, it becomes like your assistant Project Manager.

3) CoPilot In Whiteboard:

This software package does exactly as its title implies. But rather than using the traditional wall mounted whiteboard and the dry erase markers, it is all done virtually. With CoPilot being used here, you can ask it to create diagrams and other sorts of visuals, and it can even capture the ones that are most important for your project, for future reference.

4) CoPilot In Windows:

   At this level, it helps you to make sure that either your Windows 10 or 11 OS is running at peak condition, and remains fully optimized at all times. A big benefit here is that CoPilot can be used to keep up with the latest Microsoft Patch Updates.

5) CoPilot In Security:

   This is a different version of CoPilot, in that it is designed mainly to protect your Windows 10 or 11 OS, or even your Azure cloud deployment. It will detect any unusual patters of network activity that originates from your device, and can even help to mitigate the risks of you becoming the next victim of a Cyberattack.

CoPilot For Security And Cybersecurity

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:

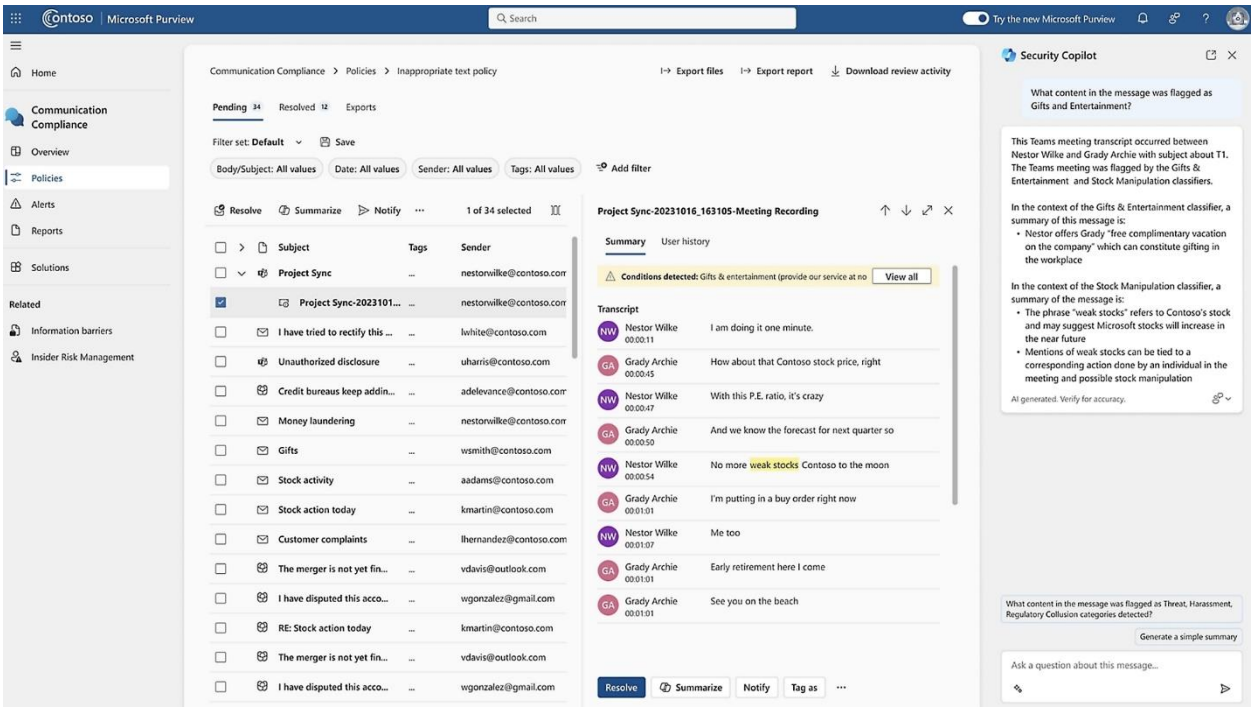
  When it comes to this, this is a huge area in which CoPilot For Security can help you with. Here are some examples:

  *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: 2).

What Is The Microsoft Purview?

Another new tool that is available from Microsoft is called “Purview”. Essentially, it has many functionalities to it that allows you to monitor and manage the datasets that are used by the AI applications that you create and store in your Azure Cloud Deployment. We will review this in more detail.

What It Is All About

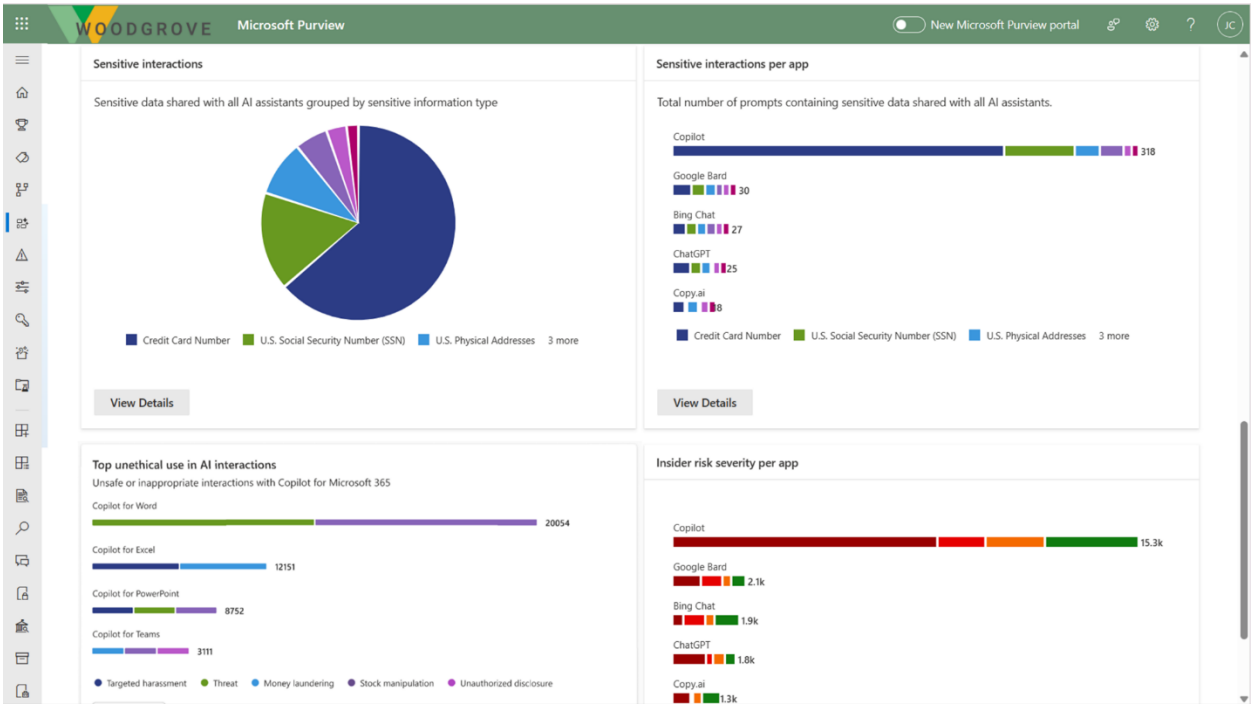
In s nutshell, Purview can be considered as a unified governance system that allows you to manage all of your datasets whether it is all in the Cloud, On Prem, or even in a Hybrid like environment, where part of your IT/Network infrastructure is in a Private Cloud, and the other is at the physical site of your business. You can get all of this from one unified view, with the following functionalities:

- You can get a birds eye view of all of your datasets, as well as a version of history of how the data was collected and used. You can even utilize the mapping function to see the location of where all of your database servers are located at. The advantage of this is that if you are ever asked

about the location of your datasets by a regulator and/or auditor, you will be able to answer them in a matter of minutes.

- Hire data specialists to manage your datasets on a real time basis, following the principles of Least Privilege and Privileged Access Management (PAM).
- Even allow your own customers to view their own data sets, with of course the right access being granted (most likely this will just be read level permissions).

All of this can be seen in the illustration below:



(SOURCE: 3).

The Functionalities of Microsoft Purview

The following are also available in Purview:

1) <u>The Data Map</u>:

   As mentioned earlier, this gives you access to all of your data sets from one dashboard. This includes the following:

   *You can capture the data about your datasets (which is technically known as the “Metadata”);

   *The Data Map is updated on a real time basis, even as more data is being ingested into your VMs and VDs;

   *Owners of datasets (such as your customers and employees) can custom create their own views in order to see what they want about their PII.

2) <u>The Data Catalog</u>:

*With this particular functionality, you can categorize and classify data into various formats, but which are also compatible with the data privacy laws.

*You can create a glossary or even a dictionary about your datasets, which also allows for tagging.

*Also, a detailed version history is kept of the datasets, from when it was first inputted into your systems to what happened to it most recently. Through the custom configuration of the views, data owners can see as much or as little information as they desire to.

3) The Data Estate Insights:

This tool has been designed specifically for the Chief Data Officers, and the other Data Stewards that help to manage the datasets. From here, these individuals will be able to keep a closer eye on malicious behavior that is happening to the PII information and data, and make sure that holes or vulnerabilities found in them are quickly remediated. In a way, these specialists can also serve as a back up to the already burdened IT Security teams.

4) The Data Sharing:

The sharing of PII datasets and other pieces of confidential information has always been a huge security risk for companies. But given the digital world that we live in today, sharing this has almost become a must. Therefore, Purview has functionalities that are embedded from within it allow for the safe and encrypted transfer from one party to another. This tool also allows you to centrally manage all of your datasets, and immediately terminate any sharing rights if anomalous behavior is detected.

The Microsoft Purview AI Hub

Another component of Purview is known as the "Purview AI Hub". The technical definition of it is as follows:

"Microsoft Purview to mitigate and manage the risks associated with AI usage, and implement corresponding protection and governance controls."

(SOURCE: 4).

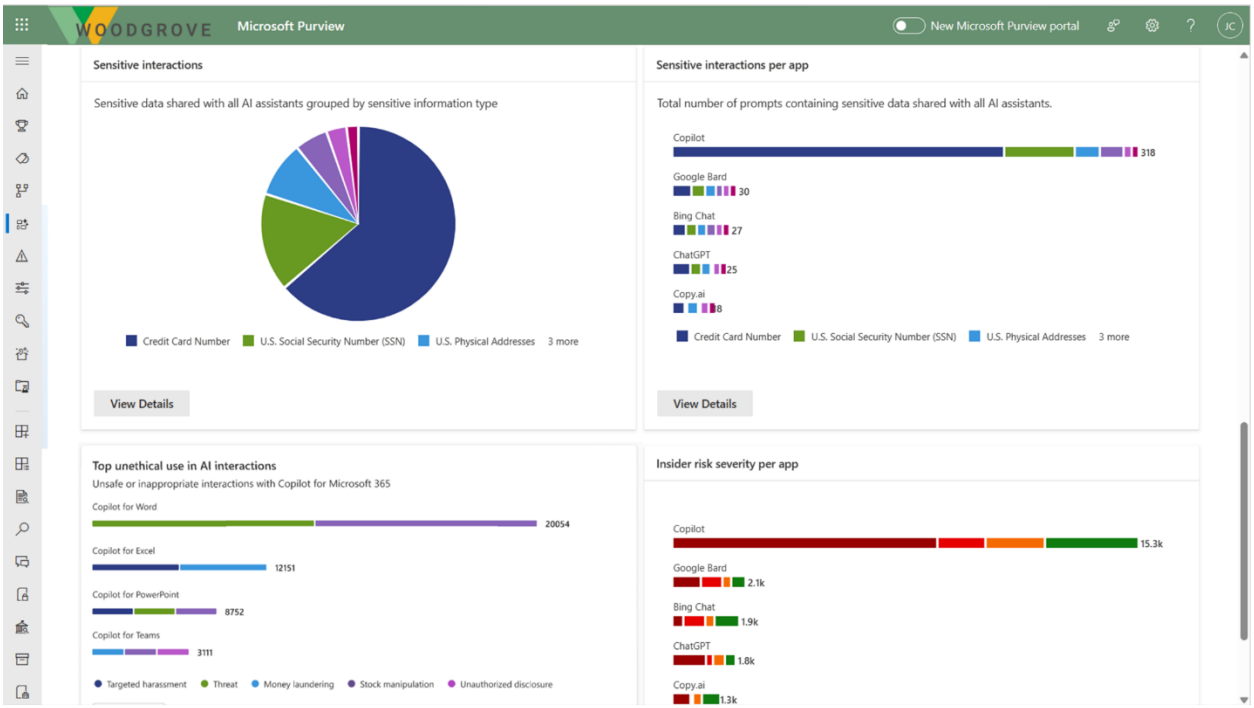
In other words, it is an all-encompassing tool deployed into your Azure Cloud Environment so that you can keep a visual eye on what is happening with all of the AI based applications that run from within it. From there, it will allow you to into compliance easily comply with the data privacy laws, of which AI is now a large part of.

It comes with the following functionalities:

- Sensitivity label creation.
- Data classification creation.
- Auditing features.
- Content search for the outputs created by your AI apps.
- eDiscovery for legal purposes.
- Retention and deletion, based upon the data privacy law(s) that your company is bound to.

The Microsoft Purview AI Hub also integrates with CoPilot, and other third party of Large Language Models (LLMs) that you may have deployed into your Azure Cloud Environment.

An illustration of it is below:



(SOURCE: 5).

The Integration Of Microsoft Purview And Microsoft CoPilot

So far in this whitepaper, we have provided an in-depth overview into what CoPilot and Purview are all about. One of the greatest common denominators between the two of them is that they are designed to provide you with information and data to make you and your team more productive, and also provide the ability to be more proactive about the getting the tasks that need to get done ahead of schedule. In this regard, you can use both of these tools in concert with another in order to not only further enhance your Security Posture, but to also mitigate the risk of becoming a victim of a massive Cybersecurity Attack.

You can use them in two different ways, which are as follows:

1) Copilot in Microsoft Purview Embedded Experiences:

   With this tool, CoPilot is actually embedded into Purview. This is what you would use to help shore your lines of Cyber Defenses.

2) Copilot in Microsoft Purview Standalone Experience:

This is an actually a standalone tool, and works in ways similar to that of ChatGPT, but on a much more powerful level. For instance, you can directly ask it questions, and it will give answers, in a wide variety of ways, which includes text, audio, images, video, etc. But, it is important to note that it focuses primarily on the datasets that you are using for AI applications that you have created and are hosting in Microsoft Azure.

We will review these in both in more detail in the next two subsections.

Copilot in Microsoft Purview Embedded Experiences

Using this, you can accomplish the following:

- Data Loss Prevention:

  Using the features that are available in Microsoft Azure, you can help to insure that your AI Apps are as fortified as possible in order to mitigate the risks of Data Exfiltration Attacks from happening. By using these tools and the strategies that you create, this is collectively known as "Data Loss Prevention", or "DLP" for short. It can be technically defined as follows:

  "Data loss prevention is a security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data. It can help your organization monitor and protect sensitive information across on-premises systems, cloud-based locations, and endpoint devices. It also helps you achieve compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR)."

  (SOURCE: 6).

  Some of the best practices for a DLP program include the following:

  *Identify and classify sensitive data.

  *Make use of data encryption.

  *Implement your DLP strategy and solution in phases, don't do this all at once.

  *Implement a patch management strategy.

  *Follow the concepts of Least Privilege, Privileged Access Management, Role Based Access Control (also known as "RBAC").

  *Try to automate the routing tasks as much as possible, by making use of Generative AI.

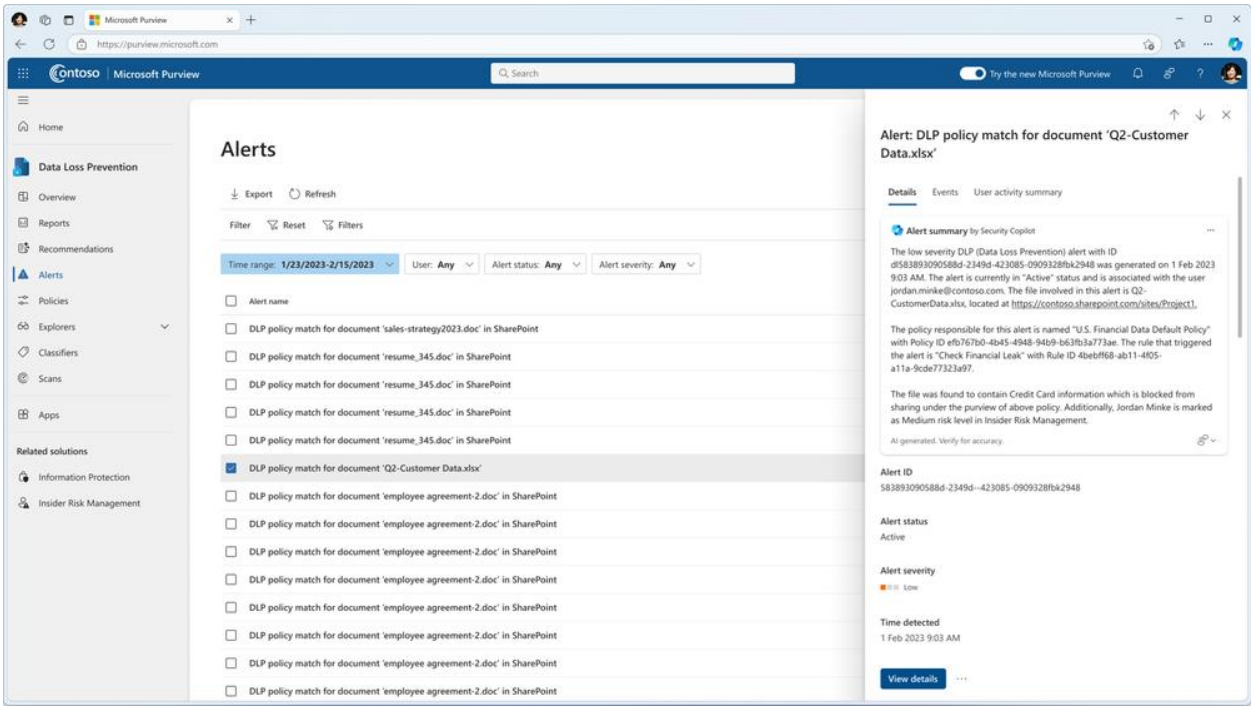
  *Use anomaly detection to detect any unusual or anomalous types of network traffic behavior.

  *Establish Key Performance Metrics (also known as "KPIs") to make sure that your DLP strategies and solution remain optimized at all times.

  Equally important is to create alerts and warnings on a real time basis, to alert you of any potential Data Exfiltration Attack that could occur. With this "Embedded" tool, this is very easy and quick to deploy. For more information on this, click on the link below:

https://learn.microsoft.com/en-us/purview/dlp-alerts-dashboard-get-started?tabs=purview#investigate-a-dlp-alert

An example of using CoPilot and Purview together to create your DLP strategies and solution is illustrated below:



(SOURCE: 7).

- Insider Risk Management:

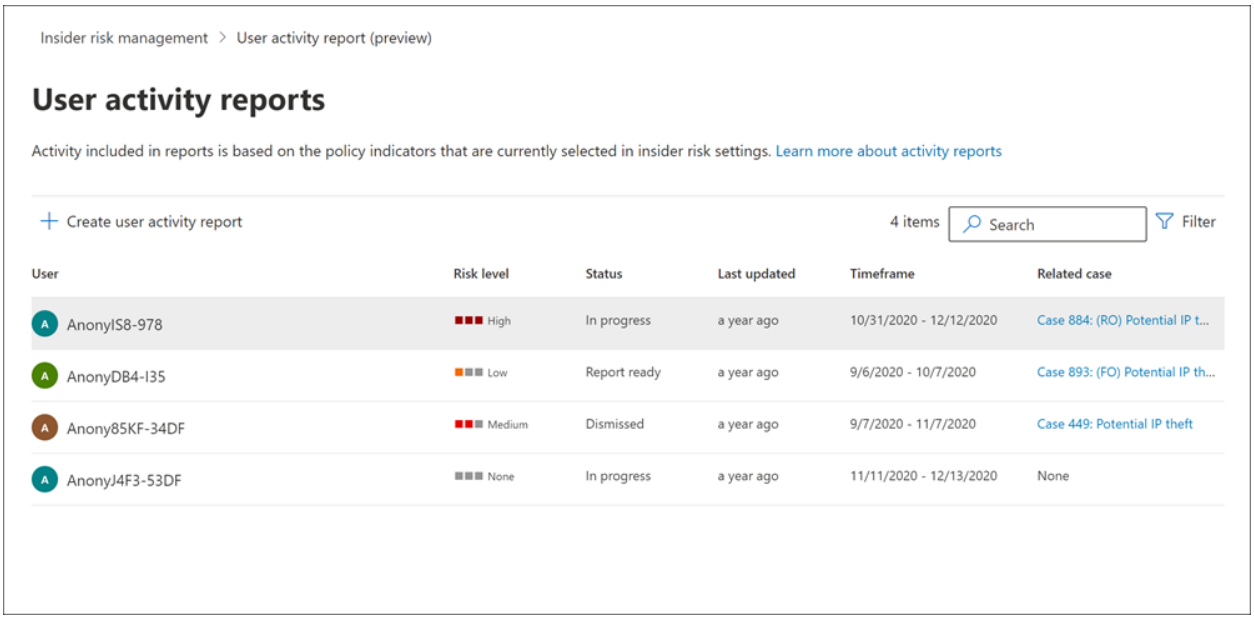
This is probably of the greatest areas in which this platform can be of an asset to your business. The term "Risk Management" is a very broad one, and it can have different kinds of connotation associated with it, depending upon the industry you are talking about. But as it relates to Cybersecurity, it can be technically defined as follows:

"Cyber risk management, also called cybersecurity risk management, is the process of identifying, prioritizing, managing and monitoring risks to information systems."

(SOURCE: 8).

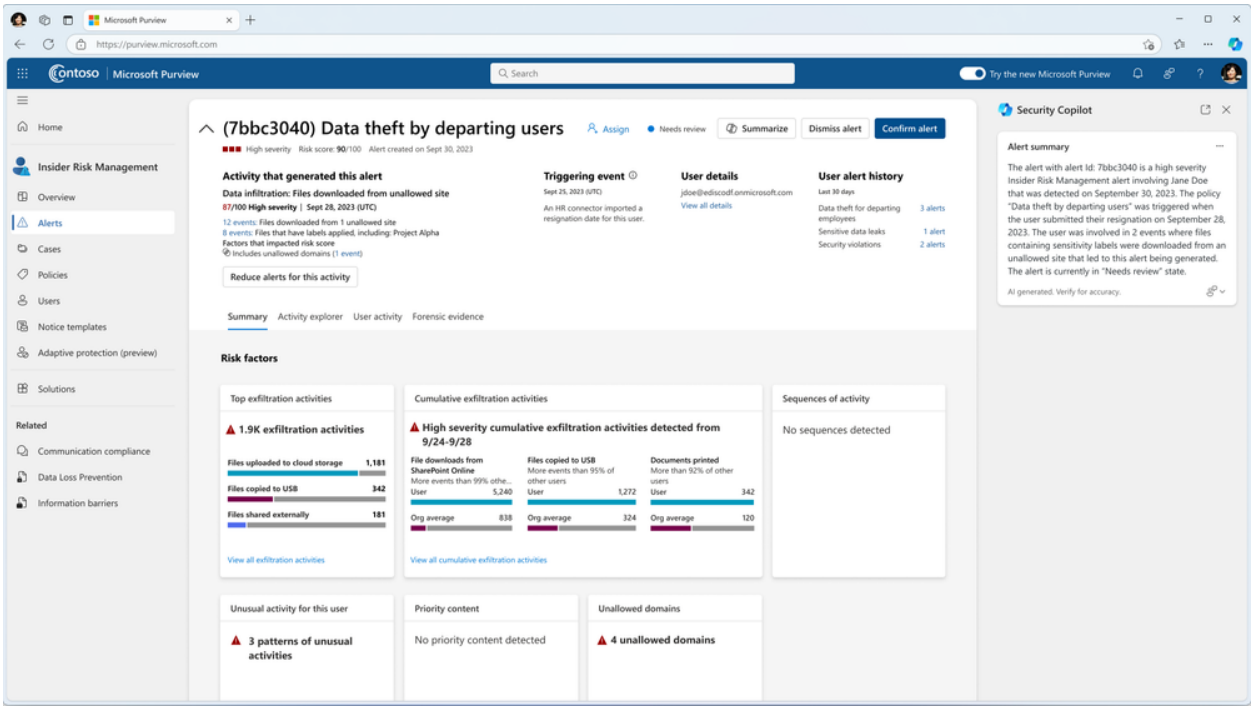
While CoPilot can actually organize and show you all of the alerts that are coming to you from all of your network security devices, it is Purview that actually help you triage them. So, when the two are used together, you and your IT Security team can be assured that your should be greatly mitigated from any security breaches happening.

Below is an illustration of how CoPilot can organize and actually show you the alerts that are received:



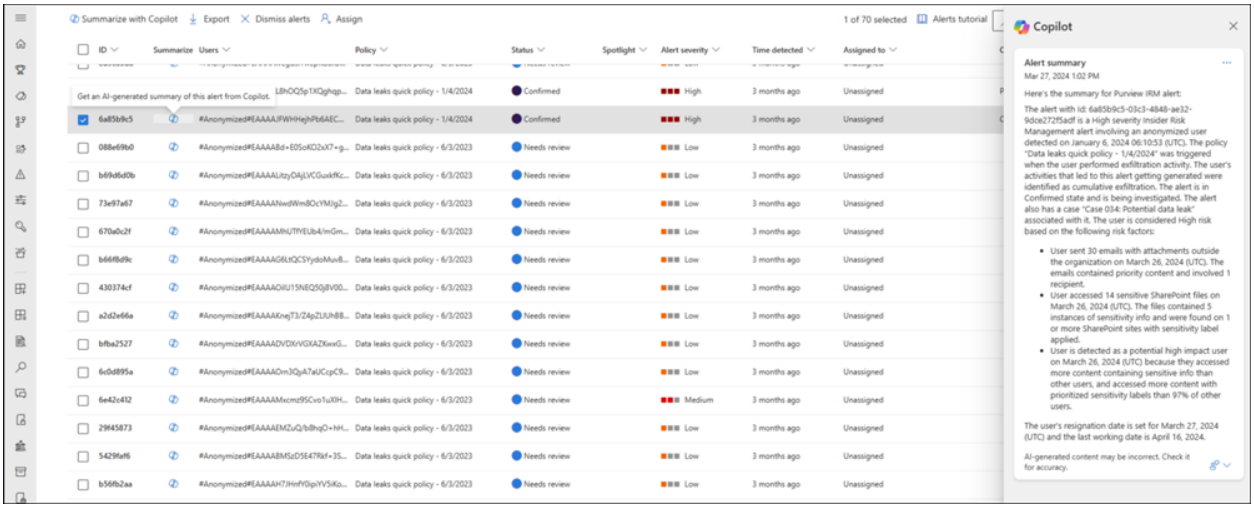
(SOURCE: 9).

Also, CoPilot will provide a detailed review of each alert, if you choose this functionality. An example of what is presented can be seen in the illustration below:



(SOURCE: 7).

How Purview can triage these alerts in terms of their degree of severity is also illustrated below:



(SOURCE: 9).

You should take the following steps when using Purview for triaging purposes:

1) Log into the Purview Portal: purview.microsoft.com

2) Go to the "Insider Risk Management Solution".

3) In the left navigation pane, select "Alerts".
4) An "Alerts Dashboard" will now appear.

5) From the above, select the alert that you think needs to be triaged immediately.

6) From the "Alerts Details" page, you can do the following:

*Confirm the alert.

*create a new triaging case.

*confirm the alert, and even add it to an open case.

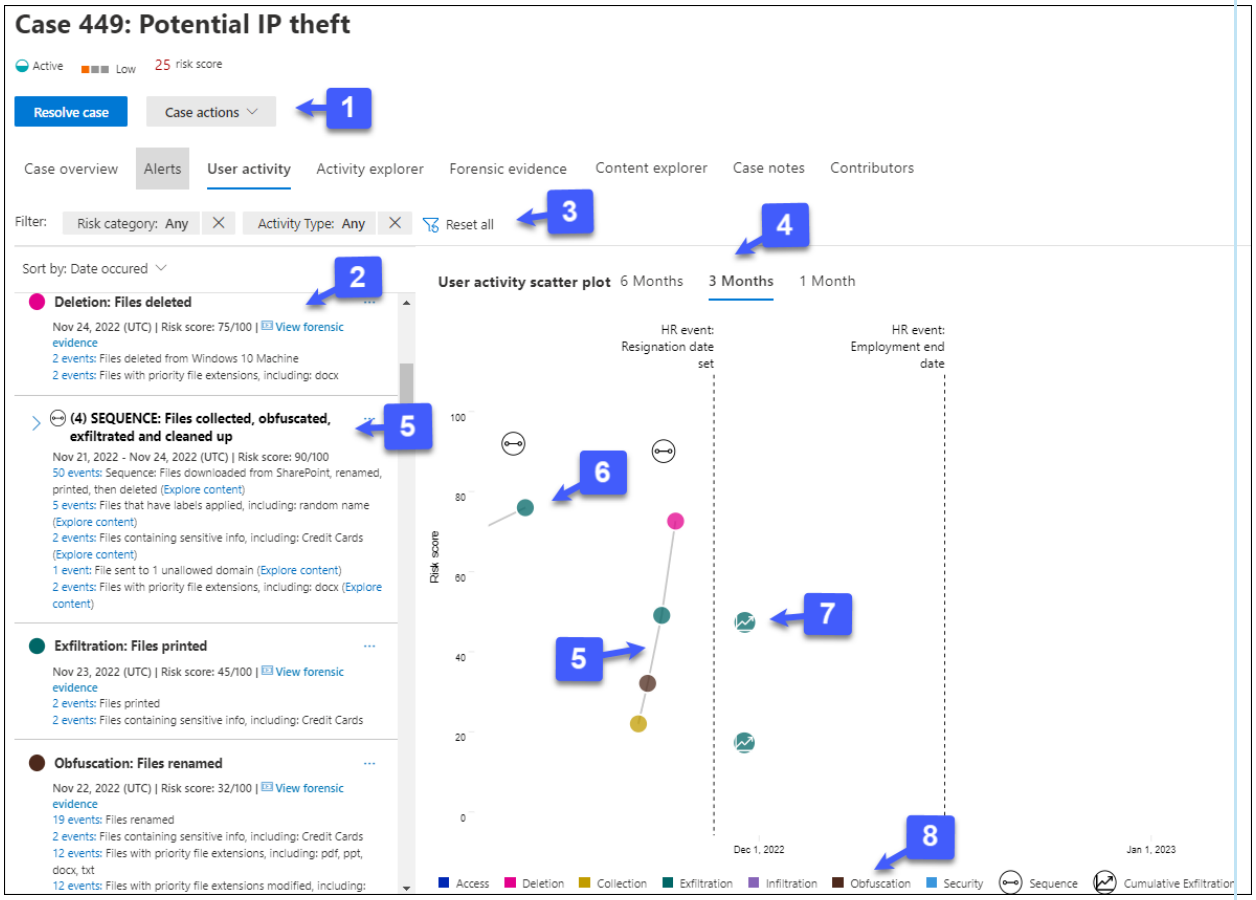
*Dismiss and cancel the alert.

*See the current status for the alert on a real time basis.

*Establish the alert risk severity level as "High", "Medium", or "Low".

It is important to note that severity level that you assign to an alert could very well increase or decrease over time if it is not addressed in time.

If you have been impacted by a Cyberattack, once you have established the mission critical operations, one of the next major activities that you will want to engage in is a Digital Forensics examination. In this regard, this embedded platform can provide invaluable information and data to aid the entire investigation process. This is illustrated in the diagram below:



(SOURCE: 9).

The numbers in the above illustration are represented by the following:

#1→ The Case Actions that have been taken.

#2→ The chronology of the Risk Activity that are associated with the alert.

#3→ Filter and Sorting for the following: Risk Category; Activity Type; Sort By.

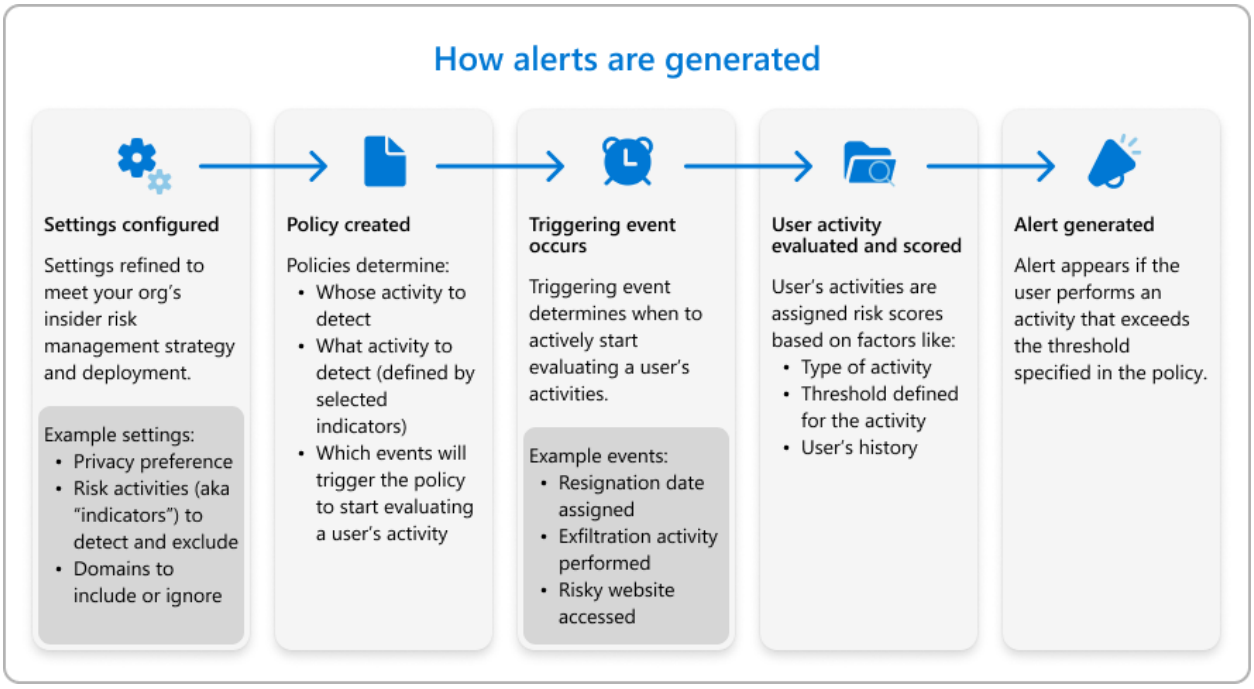
#4→ Time Filters for sorting and seeing the different stages in which the alert went through.

#5→ The Risk Sequence, which is an examination of the activities that led the alert to be created in the first place.

#6→ The Risk Activities and details that are associated with the alert.

#7→ The Risk Activity Legend, which is simply a color-coded legend which you can use as a reference for all of the Risk Activities that are associated with the alert.

The illustration below summarizes how the Embedded Platform creates the alerts, which are fed into CoPilot, then subsequently Purview:



(SOURCE: 9).

More details about how you use the Insider Risk Management Functionality can be accessed at the link below:

https://learn.microsoft.com/en-us/purview/insider-risk-management-activities?tabs=purview-portal#use-the-copilot-button-to-summarize-an-alert

- Communications Compliance:

For any business, getting into line with the Federal Regulations and Mandates is now a must, especially with the Data Privacy Laws, such as those of the GDPR, CCPA, etc. However, there is still a great deal of confusion as to what "Compliance" is really about. As it relates to Cybersecurity, it can be technically defined as follows:

"Cybersecurity compliance refers to adhering to standards and statutory requisites set by entities, law or governing bodies. Companies handling digital assets need to implement controls and security practices to minimize the risk to sensitive data."

(SOURCE: 10)

As you can see from the above definition, Cyber Compliance is primarily twofold:

*Ensuring that the right controls are put into place to protect the datasets from an Exfiltration Attack.

*In turn also ensuring that you brand and reputational image remains strong even after a Cyberattack, by coming into line with the data privacy laws, as just previously mentioned.

In this regard, the Embedded Platform can help you and your IT Security team to achieve the above two objectives, and much more. For example, much of the processes are now automated when it comes to reviewing Compliance Alerts, Compliance Reports, etc. with the end result of coming to a resolution on any open cases. One of the main advantages to this kind of approach is that you will have both a record and audit trail that can be presented to a regulator of a data privacy law in case your business is ever audited by one.

With the Embedded Platform, a majority of this is now being down with what is known as "Prompt Engineering". This is where you simply enter in the right keywords in order to find exactly what you are looking for, in this case it would most likely be a Compliance Report that needs further investigation in order for it to be fully resolved.

One of the most important and useful functionalities that you will find by using the Embedded Platform is for the quick filtering of Compliance Reports. Before you can start to search for Compliance Reports, you first need to configure the Filtering mechanism. To do this, follow these steps:

1) Log into the Purview Portal: purview.microsoft.com

2) Navigate to the to the "Communication Compliance" solution.

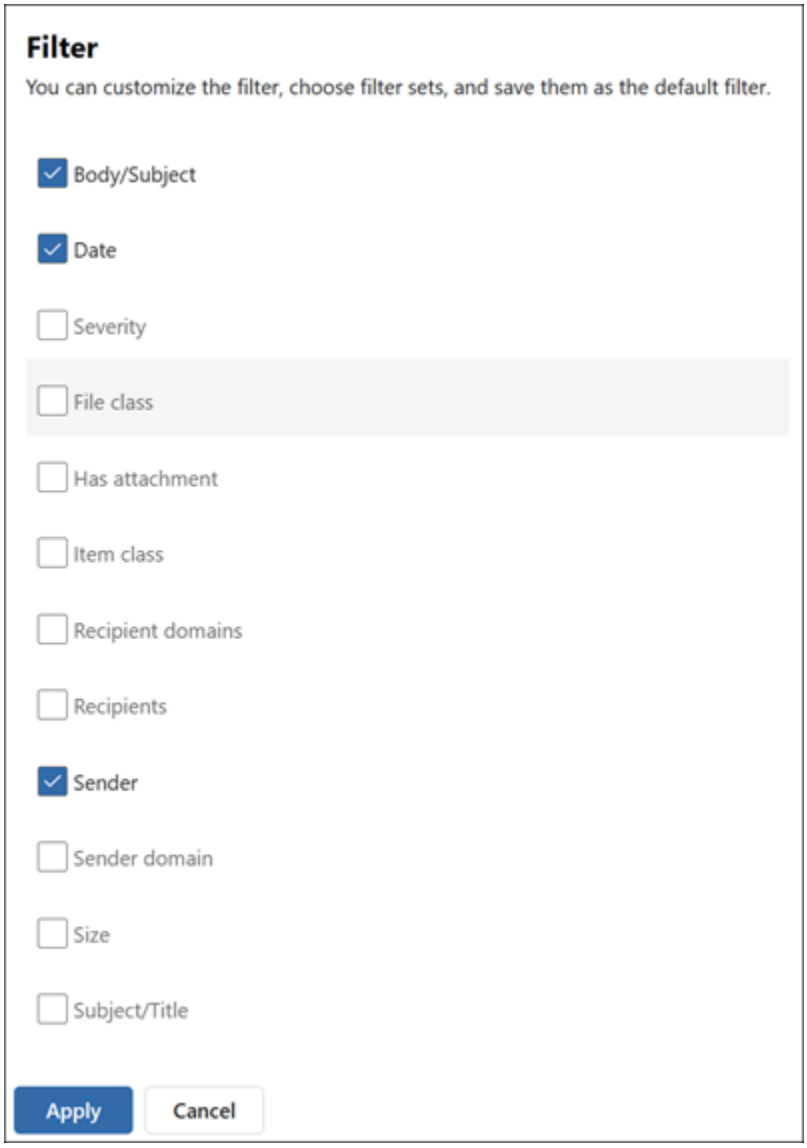
3) In the left navigation pane, select "Policies".

4) On the above page, select either the "Pending" or "Resolved" tab to display the items for that you want to filter for.

5) Select the "Filters" button.

6) Select the appropriate "Filter For" checkboxes, when you are done with that, select "Apply".

7) To save what the Filter Query for future uses, , select the "Save The Query" button. Also make sure to enter a specific name for the Filter Query. This is illustrated below:

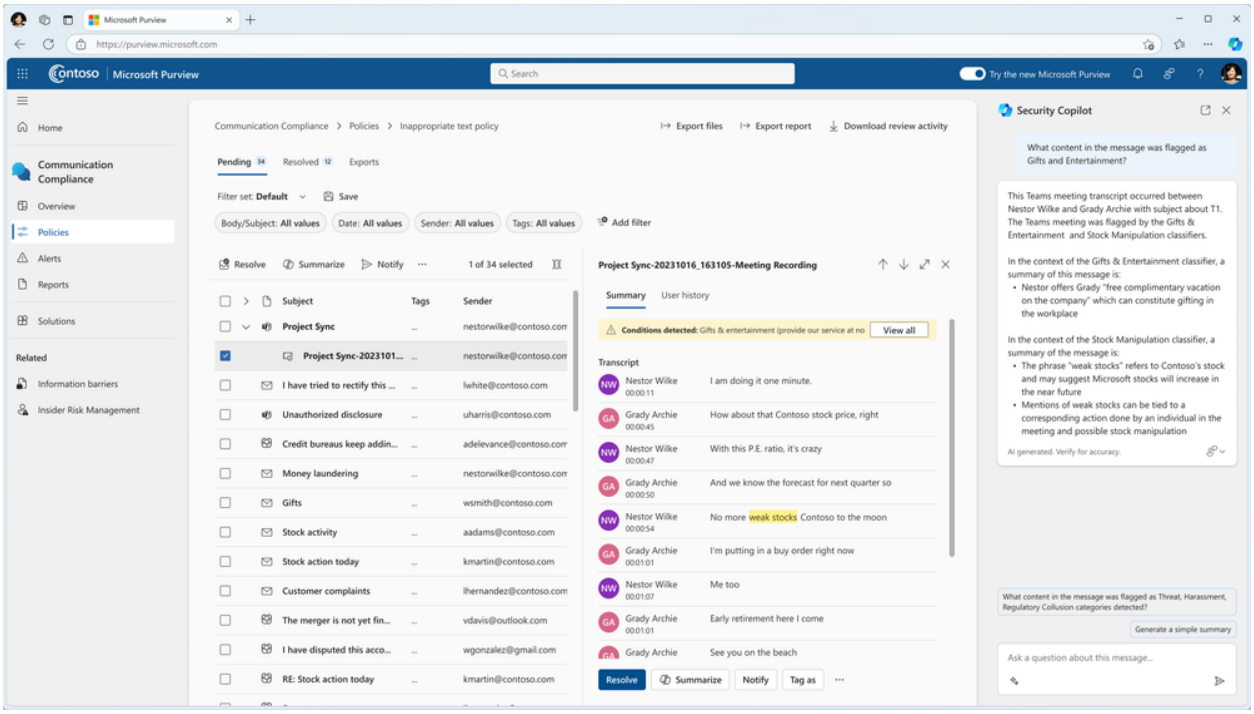


(SOURCE: 11).

For more details, and how to automate the Compliance process by using Prompt Engineering, click on the link below:

https://learn.microsoft.com/en-us/purview/communication-compliance-investigate-remediate?tabs=purview-portal#summarize-a-message-by-using-copilot-in-microsoft-purview

If the need ever arises, you can also get a holistic view of all of the Compliance Reports that the Embedded Platform has created. This is illustrated below:



(SOURCE: 7).

- E-Discovery Cases:

One of the most powerful assets (along with many others) that any M365 possesses are the eDiscovery tools. A technical definition of eDiscovery is:

"eDiscovery is the process of finding and collecting electronic data for use in legal proceedings. The data can be stored anywhere, including on computers, servers, email systems and cloud-based storage systems. Once retrieved, you might then need to deliver the data as evidence."

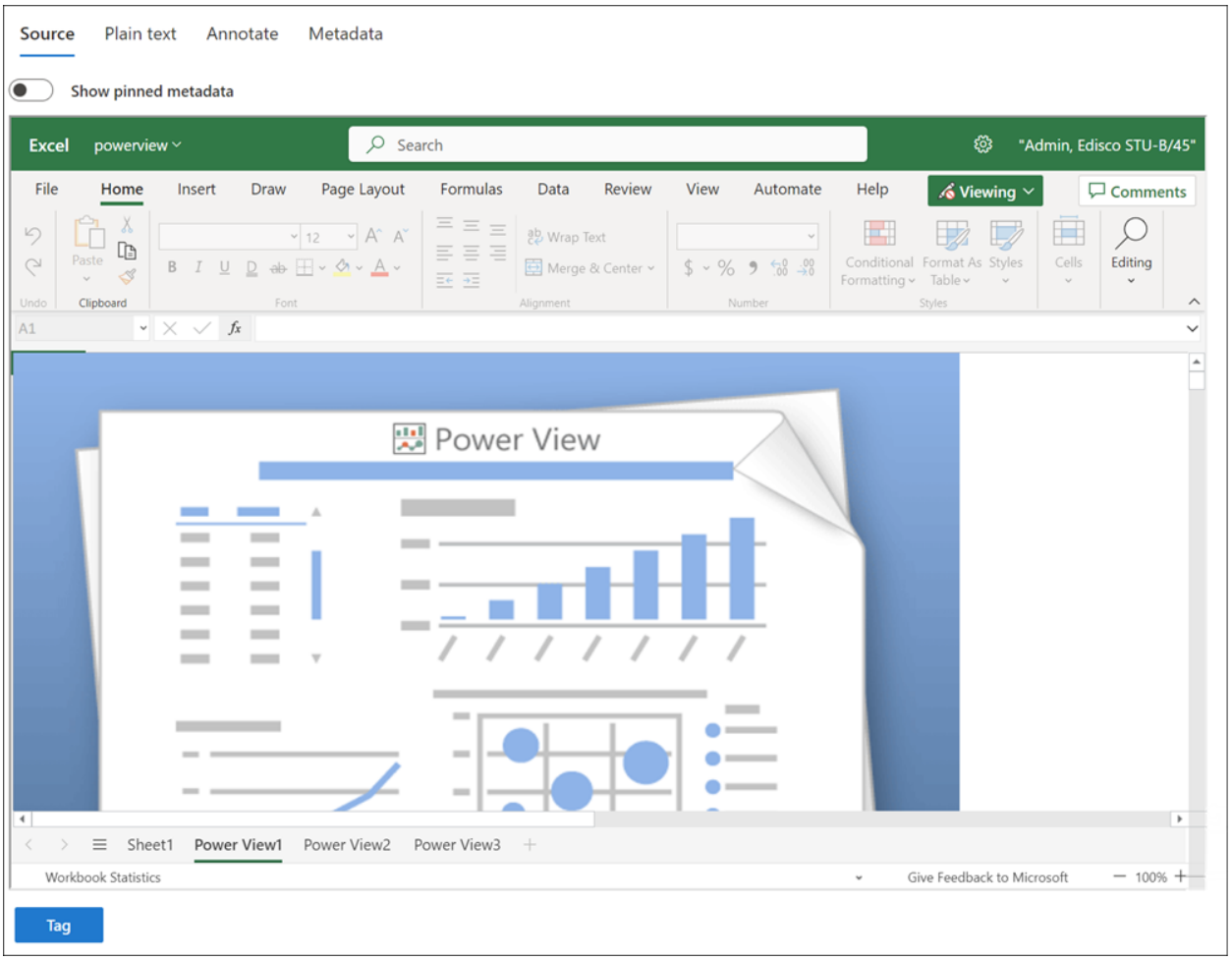
(SOURCE: 12).

When you are searching for documents that can be used for evidence, the Embedded Platform gives you four different choices in how it can be presented. They are as follows:

*The Source View:

This option is the best view of a selected document. It can support hundreds of file types, ranging from Microsoft Office files, Microsoft Teams chats, Excel formulas, and PowerPoint notes.

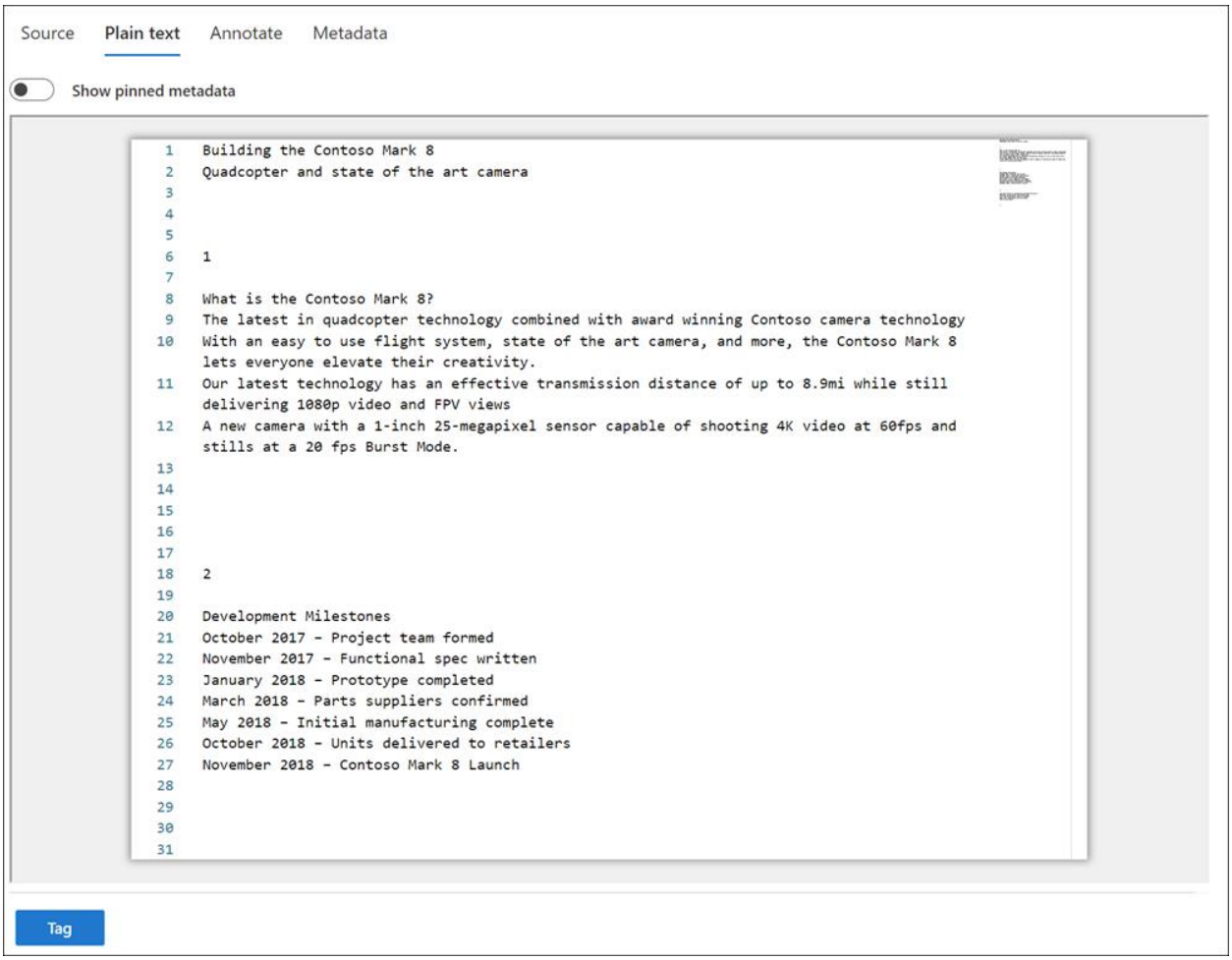
An example of this is illustrated below:



(SOURCE: 13).

*<u>The Plain Text View:</u>

This option provides a view of extracted text of any file that you select. But, as its name implies, images and formatting are not included, but the advantage of this is that it allows you to understand content quickly. It also includes a line counter so that you can make notations in the text, and you can conduct quick keyword searches using the scrollbar. An example of this is illustrated below:



(SOURCE: 13).

*<u>The Annotated View</u>:

This option is used primarily to apply markup on a selected document. Some of these include:

→Select annotations: mark certain pieces of content to be deleted.

→Select text: Select any text for further viewing.

→Area redactions: Draw a box around sensitive content to hide it.

→Pencil: With your hand, highlight certain areas of the content.

→Toggle annotation transparency: This will make selected pieces of content to appear “hidden”, but not redacted.

→Previous page: Go to the previous page.

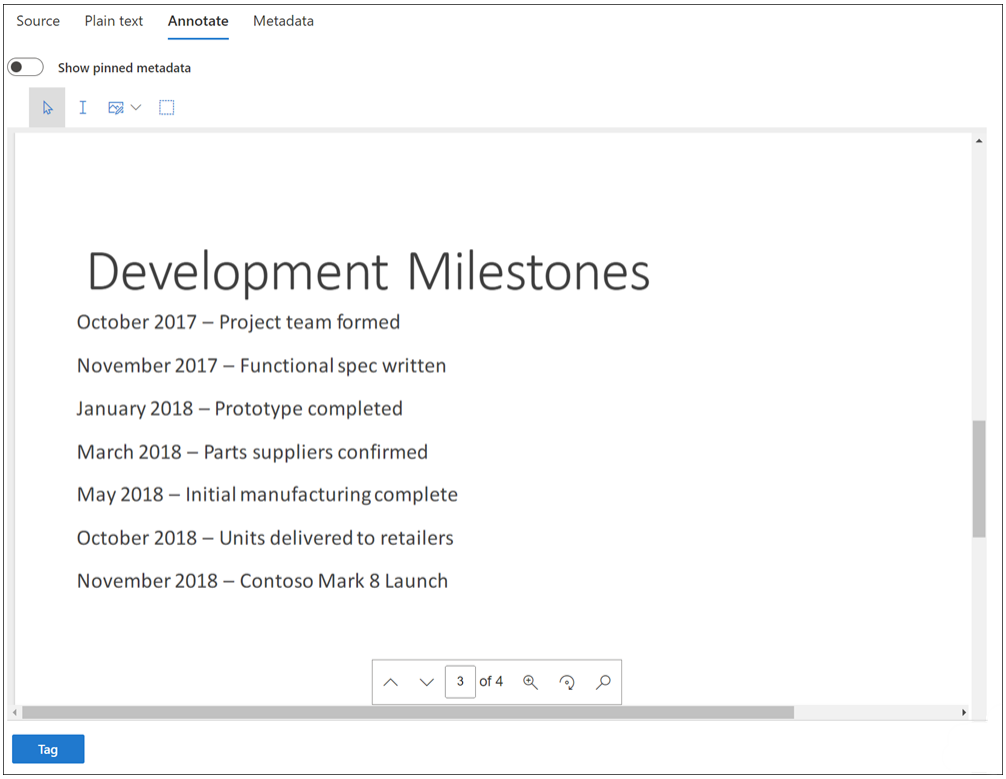
→Next page: Go to the next page.

→Go to page: In the search box, type in page number to navigate to.

→Zoom: Set the zoom level for annotated view.

→Rotate: Rotate the document by 90 degrees, 180 degrees, or 360 degrees.

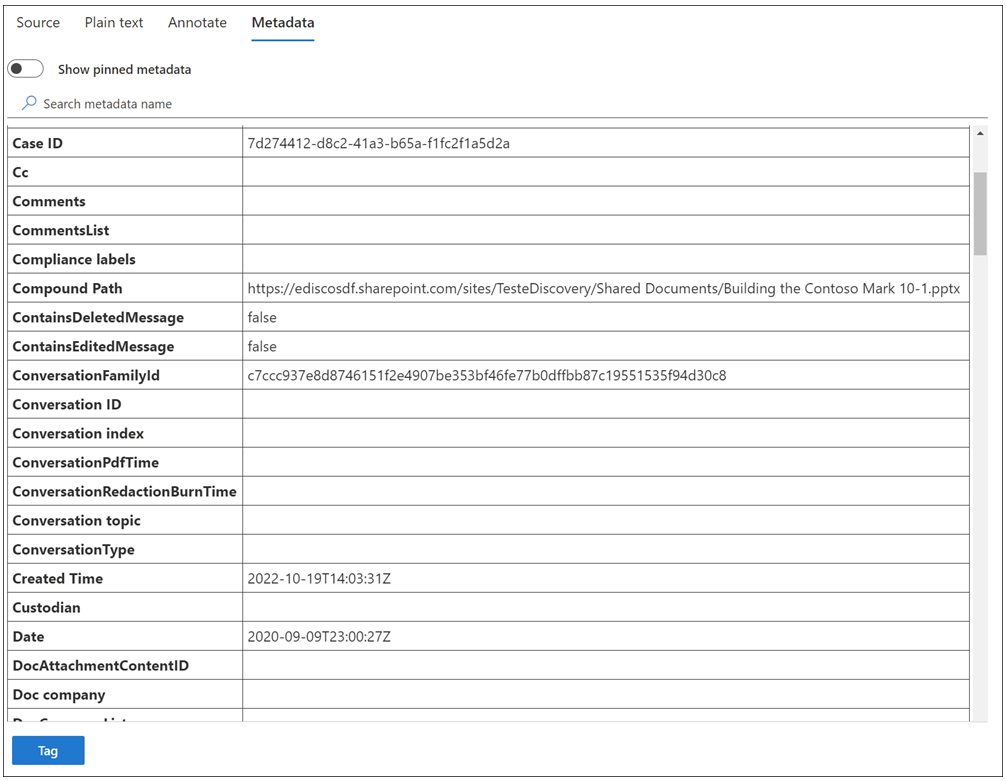
An example of this is illustrated below:



(SOURCE: 13).

*<u>The Metadata View</u>:

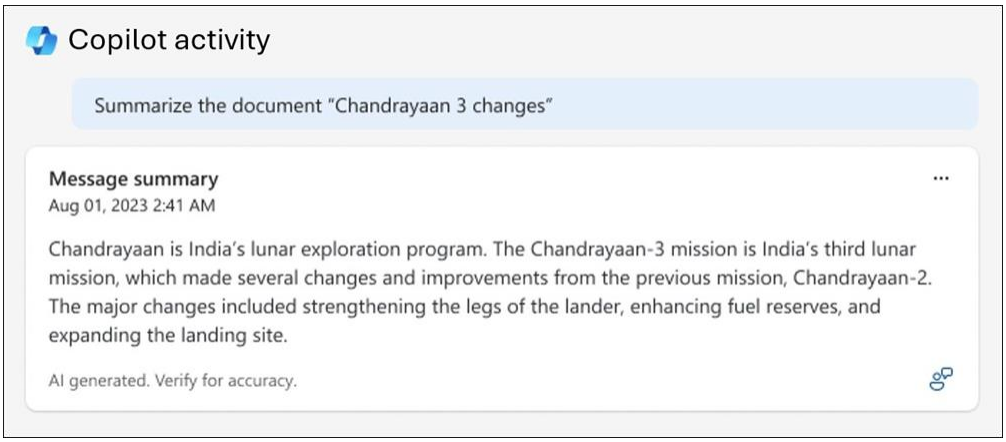
This option allows you to view "the data about the data" that resides in the document. For example, Metadata panel can be used to an be toggled on or off to display the various metadata. An example of this is illustrated below:



(SOURCE: 13).

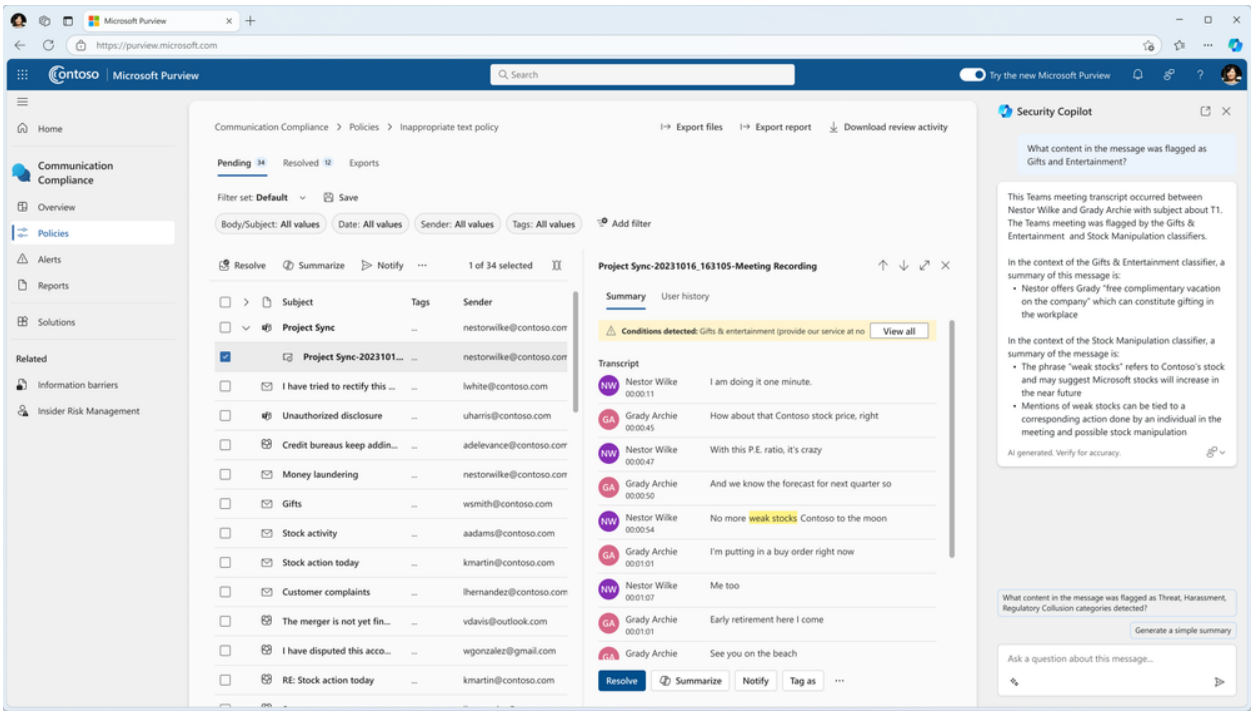
*<u>The CoPilot View</u>:

Using this option, you can use Prompt Engineering to search for exactly those documents that you need for your eDiscovery case. An advantage of this is that since Generative AI power it, you can also get a "Contextual Summary" as well. An example of this is illustrated below:



(SOURCE: 13).

An example of the Contextual Summary that can be generated is illustrated below:



(SOURCE: 7).

An example of how Prompt Engineering is used in this regard is illustrated below:

For more details on how to use eDiscovery with the Embedded Platform, click on the link below:

https://learn.microsoft.com/en-us/purview/ediscovery-view-documents-in-review-set#copilot-activity-view

Copilot in Microsoft Purview Standalone Experience

With this tool, not only can get most of the functionalities from the Embedded Platform, but there is also a special emphasis on the use of what are known as "Promptbooks". This can be technically defined as follows:

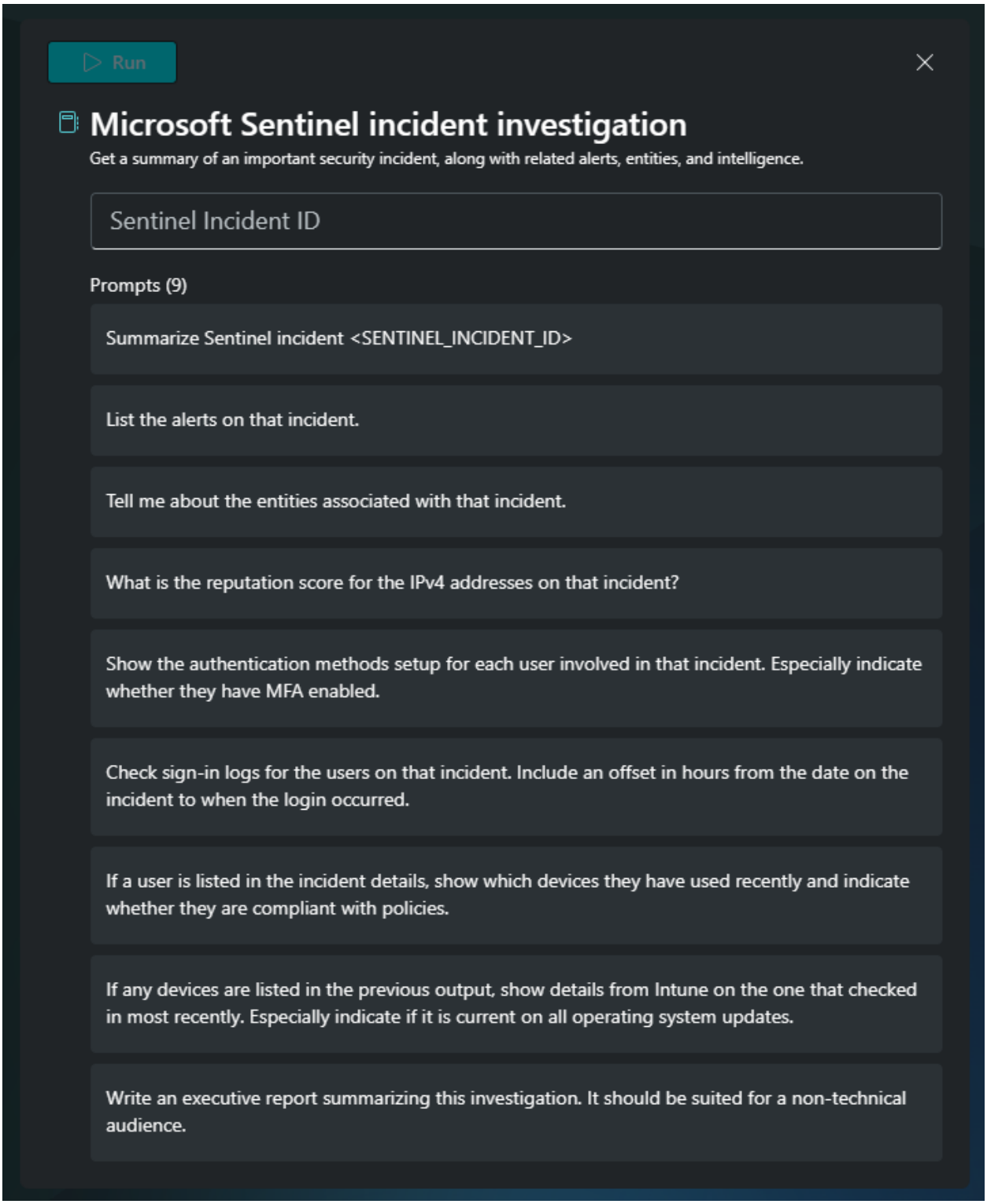
"[It is] a series of prompts that have been put together to accomplish specific security-related tasks. They can function in a similar way as security playbooks—ready-to-use workflows that can serve as templates to automate repetitive steps—for instance, with regard to incident response or investigations. Each prebuilt promptbook requires a specific input (for example, a code snippet or a threat actor name)."

(SOURCE: 14).

Examples of various Promptbooks are covered in the next four subsections:

- The Security Breach Investigation:

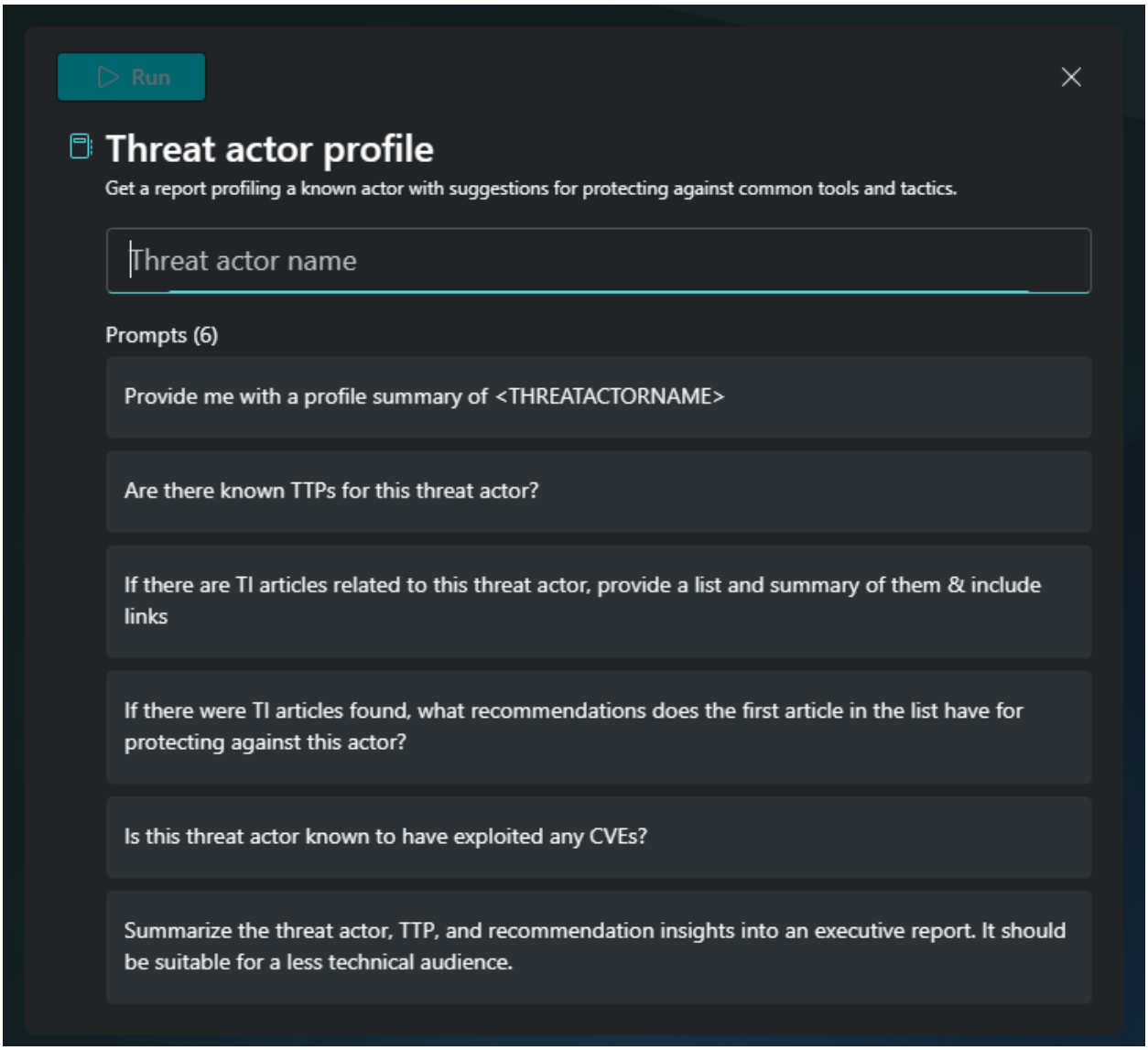
  With this, you are primarily using either Microsoft Defender, or its associated XDR plug in. This is illustrated in the example below:


Run
Microsoft Sentinel incident investigation
Get a summary of an important security incident, along with related alerts, entities, and intelligence.
Sentinel Incident ID
Prompts (9)
Summarize Sentinel incident <SENTINEL_INCIDENT_ID>
List the alerts on that incident.
Tell me about the entities associated with that incident.
What is the reputation score 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.
Check sign-in logs for the users on that incident. Include an offset in hours from the date on the incident to when the login occurred.
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.

(SOURCE: 14).

- The Theat Actor Profile:

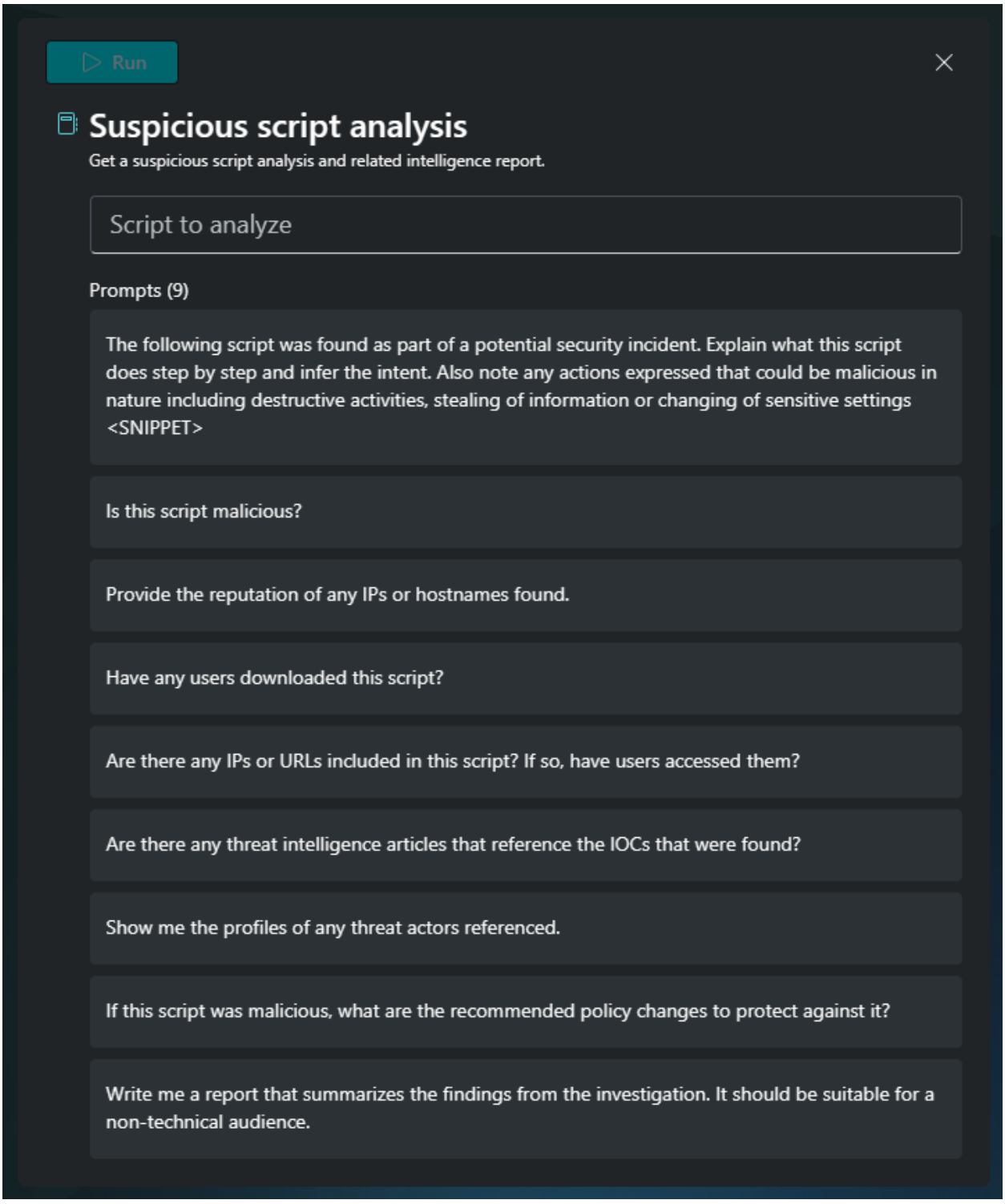
  You can use this option to any existing threat intelligence about the actor, including known tools, tactics, and procedures (TTPs) and related items. Also, corrective actions for remediation are also provided. It can also create a report that is non-technical in nature, so that all intended recipients can easily understand it. An example of this is illustrated below:



  (SOURCE: 14).

- The Suspicious Script Analysis:

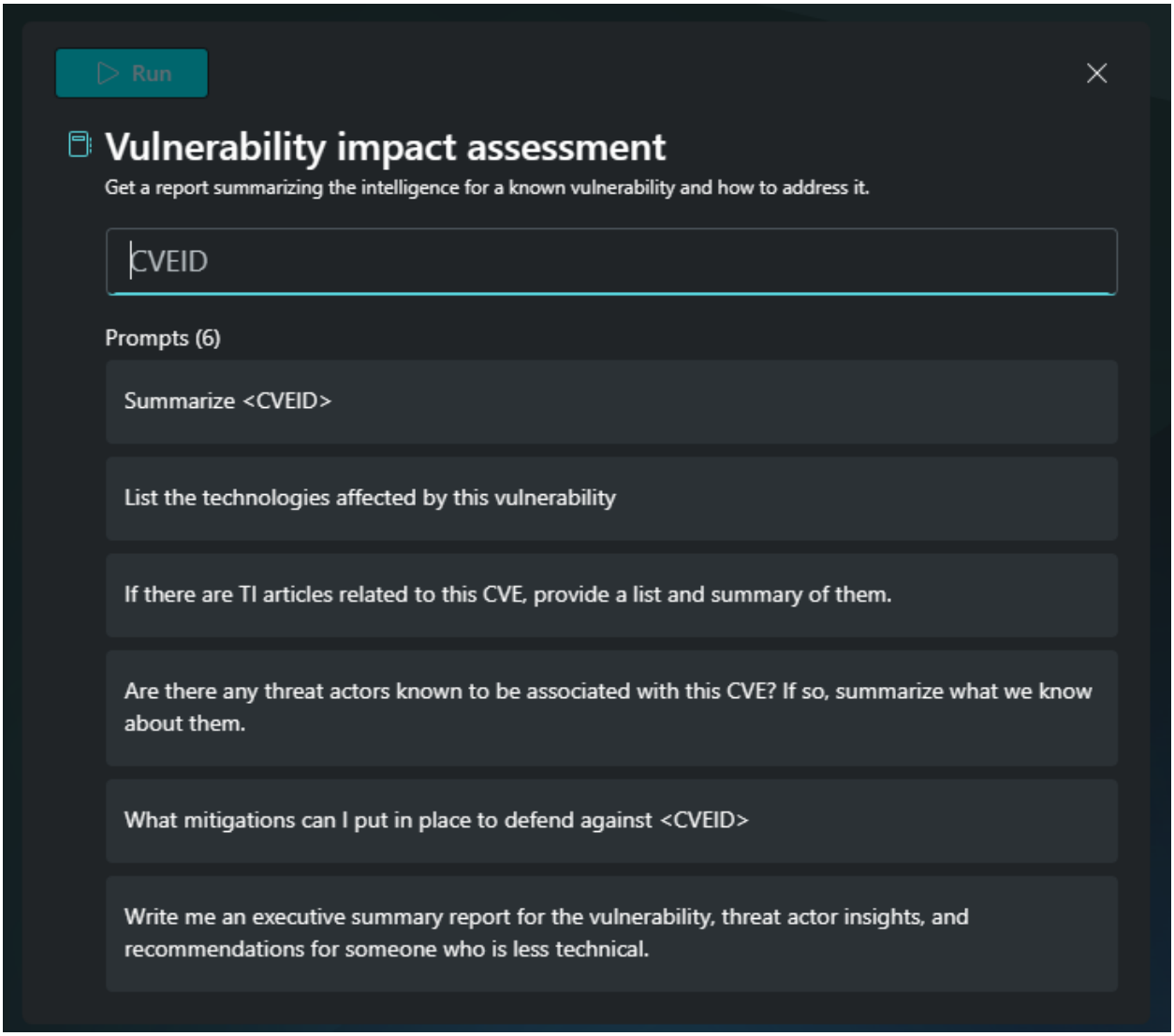
  This option can be used to examine any backdoors that have been left behind in the scripts that have been created by PowerShell or the Command Line in the Windows Operating System. An example of this is illustrated below:



(SOURCE: 14).

- The Vulnerability Impact Assessment:

With this option, you can enter in a CVE (this is an acronym that stands for “Common Vulnerabilities and Exposures”) number or even a name of a known vulnerability. You will then receive more information and data, and from there, recommendations will be provided on how to mitigate this threat from impacting your business. You can also get a summarized report as well. An example of this is illustrated below:



(SOURCE: 14).

NOTE: More information about the CVE can be found at this link below:

https://www.cve.org/

More information about this platform can be accessed at the link below:

https://learn.microsoft.com/en-us/copilot/security/using-promptbooks#what-are-promptbooks

How To Launch Purview Into CoPilot

If you want to launch Purview into CoPilot, follow these steps:

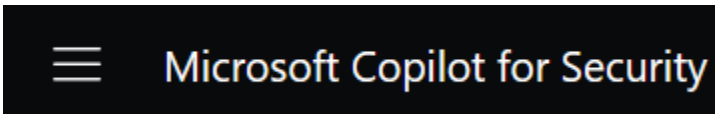
1) Make sure that you have at least “Owner Permissions” in CoPilot. For more information on how to confirm this, click on the link below:

   https://learn.microsoft.com/en-us/copilot/security/authentication#access-copilot-for-security-platform

2) Go to:

   https://securitycopilot.microsoft.com/

3) Open the “Microsoft Copilot for Security” tool bar. This is illustrated below:



   (SOURCE: 15)

4) Click on “Owner Settings”.

5) Switch this into the “On” Position: “Allow Copilot for Security To Access Data From Your Microsoft 365 Services”.

6) At the Prompt bar, click on “Sources”. This is illustrated below:

   (SOURCE: 15).

7) The “Manage Plugins Page” will now appear. From here, set the “Purview” Toggle to “On”.

8) You will now need to confirm that Purview is set up to have all of the capabilities to perform the tasks that you need it to do. To do this, click on the “Capabilities Control” button, which is illustrated below:

9) Now, select “See all System Capabilities” to see what you have. Some examples of what you should have include the following:

- “Get Data Risk Summary
- Get User Risk Summary
- Summarize Purview Alert
- Triage Purview Alerts
- Zoom into Purview Data and User Risk”

  (SOURCE: 15).

Examples Of Prompt Engineering

As was reviewed earlier in this whitepaper, Prompt Engineering is a key component when you make use of Purview and CoPilot together. For a quick tutorial on this, click on the link below:

Some examples of good Prompts include the following:

- “Show me the top five DLP alerts from the past 24 hours.
- Summarize the DLP alert with ID <12345>.
- What's the risk profile of the user that's associated with the DLP alert <12345>.
- Show me the top five Insider Risk Management alerts from the past 24 hours.
- What items did user <user> exfiltrate in the past 30 days”.

  (SOURCE: 15).

Conclusions

Apart from what was reviewed in this whitepaper, the Purview and CoPilot will also let you achieve the following for your business:

- Detect insider risk, which is the threat of unauthorized or malicious actions by employees or contractors who have access to sensitive data.
- Query for sources, schemas, classifications, and policies.
- Make recommendations for “Code Snippets: for accessing and processing data in your M365 subscription.

- Alert your IT Security team to any potential violations of data policies or best practices, such as accessing sensitive data without proper authorization or encryption.

- Enforcing your Security and Data Policies and Best Practices.

- Generating logs files and filter for certain types of data access and usage, such as who, what, when, where, and how data was accessed or modified.

If you are interested in using Purview and CoPilot together for your business, please contact us.

Sources

1) https://www.microsoft.com/en-us/microsoft-365/blog/2023/03/16/introducing-microsoft-365-copilot-a-whole-new-way-to-work/
2) https://www.datacamp.com/blog/what-is-prompt-engineering-the-future-of-ai-communication
3) https://docs.microsoft.com/en-us/azure/purview/overview
4) https://learn.microsoft.com/en-us/purview/ai-microsoft-purview
5) https://learn.microsoft.com/en-us/purview/purview-compliance-portal
6) https://www.microsoft.com/en-us/security/business/security-101/what-is-data-loss-prevention-dlp
7) https://techcommunity.microsoft.com/t5/image/serverpage/image-id/525049i303F9F7D4BA356DE/image-size/large?v=v2&px=999
8) https://www.ibm.com/topics/cyber-risk-management#:~:text=Cyber%20risk%20management%2C%20also%20called,broader%20enterprise%20risk%20management%20efforts.
9) https://learn.microsoft.com/en-us/purview/insider-risk-management-activities?tabs=purview-portal#use-the-copilot-button-to-summarize-an-alert
10) https://sprinto.com/blog/cyber-security-compliance/
11) https://learn.microsoft.com/en-us/purview/communication-compliance-investigate-remediate?tabs=purview-portal#summarize-a-message-by-using-copilot-in-microsoft-purview
12) https://www.cloudficient.com/blog/what-is-office-365-ediscovery
13) https://learn.microsoft.com/en-us/purview/ediscovery-view-documents-in-review-set#copilot-activity-view
14) https://learn.microsoft.com/en-us/copilot/security/using-promptbooks#what-are-promptbooks
15) https://learn.microsoft.com/en-us/purview/copilot-in-purview-overview