

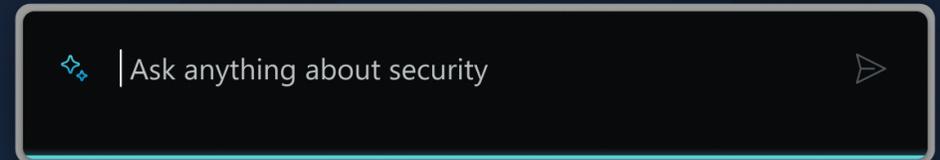


Microsoft Copilot for Security

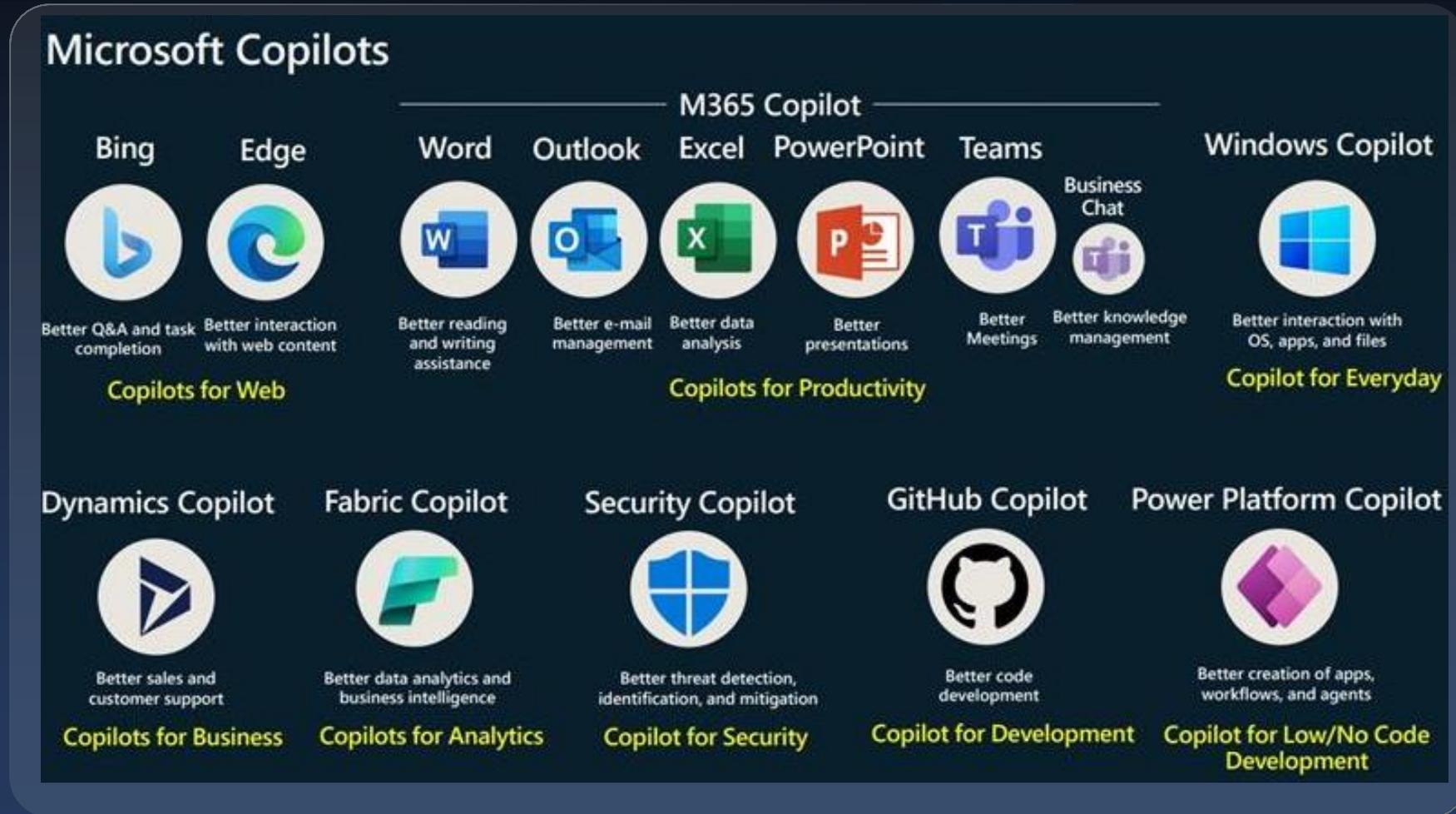


Agenda

1. Microsoft Copilots
2. Benefits of AI in Security
3. What is Copilot for Security
4. An introduction to Microsoft Copilot for security
5. Main use cases
6. How Copilot works with Microsoft security stack
7. Copilot for Security Advantage
8. Architecture and Prompts
9. Next steps



Moving away from an app-centric view



A copilot for every Microsoft Cloud experience

Amplify human ingenuity with the AI-powered future of work

- INTRODUCTION
- OVERVIEW
 - AI strategic pillars
 - Microsoft Copilot**
 - Azure AI
 - Azure OpenAI Service
 - Responsible AI
 - Foundations for AI success
- INNOVATE TOGETHER
- MARKET TOGETHER
- SELL TOGETHER

Every employee

Copilot for Microsoft 365
Works alongside you in the apps you use every day.
[Learn more >](#)

Microsoft Copilot Pro
AI-powered chat with commercial data protection.
[Learn more >](#)

Windows Copilot
The first centralized AI assistance on a platform.
[Details coming soon](#)

Functional business roles

Microsoft Sales Copilot
Maximize productivity with the AI assistant designed for sellers.
[Learn more >](#)

Dynamics 365 Copilot
Turbocharge your workforce with a copilot for every job role.
[Learn more >](#)

Security and IT professionals

Microsoft Security Copilot
Defend at machine speed with Microsoft Security Copilot.
[Learn more >](#)

Developers and data professionals

GitHub Copilot
Increase developer productivity to accelerate innovation.
[Learn more >](#)

Power Platforms Copilot
Imagine it, describe it, and Power Platform builds it.
[Learn more >](#)

Copilot for Microsoft Fabric
Infusing the power of large language models into Power BI.
[Learn more >](#)

Benefits of AI in Security – protect at machine speed

Amplify your team's impact and efficiency with guidance informed by 65 trillion daily signals.



Catch what others miss

Summarize vast data signals into key insights to cut through the noise, detect cyberthreats before they cause harm, and reinforce your security posture.



Outpace adversaries

Put critical guidance and context at analysts and admins' fingertips so they can respond in minutes instead of hours or days.



Augment team expertise

Elevate teams' proficiency as analysts and admins are empowered to perform more advanced capabilities so expert team members can be redirected to the hardest challenges.

What is Copilot for Security

Copilot for Security is a generative **AI-powered security solution** that helps increase the efficiency and **capabilities of defenders** to improve security outcomes at machine speed and scale, while remaining **compliant to responsible AI principles**.

When thinking about Copilot for Security, consider a broad reach. There are many use cases **beyond the SOC Analyst persona**.

Some include:

- IT Administrator
- Insider Risk Analyst
- Identity Access Management Administrator
- Compliance Analyst



An introduction to Microsoft Copilot for Security

Microsoft Copilot for Security (Copilot) is a generative AI-powered security platform that helps security and IT professionals respond to cyberthreats, process signals, and assess risk exposure at the speed and scale of AI, while remaining compliant with responsible AI principles.

Some of the top Copilot features are:

It can swiftly summarize information about an incident by enhancing incident details with context from data sources (e.g. data integrated from other security products or proprietary process documents uploaded to Copilot), assess its impact, and provide guidance to analysts

It can provide information on events that might expose organizations to a known threat and prescriptive guidance on how to protect against those potential vulnerabilities.

It can generate ready-to-share executive summaries, technical summaries or reports on security investigations, publicly disclosed vulnerabilities, or threat actors and their campaigns.

It can leverage the full power of OpenAI GPTs and Azure AI architecture to generate a response to a user prompt by using security-specific plugins, including organization-specific information, authoritative sources, and global threat intelligence.

It can seamlessly integrate with products in the Microsoft Security portfolio such as Microsoft Defender XDR, Microsoft Sentinel, Microsoft Purview, Microsoft Entra and Microsoft Intune, as well as other third-party services such as ServiceNow, Netskope, and Cyware.

Main Use Cases

For the initial launch of Copilot for Security, our focus was on making four primary use cases amazingly easy to use:



Incident Summarization

Gain context for incidents and improve communication across your organization by leveraging generative AI to swiftly distill complex security alerts into concise, actionable summaries, which then enables quicker response times and streamlined decision-making



Impact Analysis

Utilize AI-driven analytics to assess the potential impact of security incidents, offering insights into affected systems and data to prioritize response efforts effectively.



Reverse Engineering of Scripts

Eliminate the need to manually reverse engineer malware and enable every analyst to understand the actions executed by attackers. Analyze complex command line scripts and translate them into natural language with clear

explanations of actions. Efficiently extract and link indicators found in the script to their respective entities in your environment.



Guided response

Receive actionable step-by-step guidance for incident response, including directions for triage, investigation, containment, and remediation. Relevant deep links to recommended actions allow for quicker response.



Device management

Generate policies and simulate their outcomes, gather device information for forensics, and configure devices with best practices from similar deployments.



Identity management

Discover overprivileged access, generate access reviews for incidents, generate and describe access policies, and evaluate licensing across solutions.



Data security and compliance

Identify data impacted by security incidents, generate comprehensive summaries of data security and compliance risks, and surface risks that may violate regulatory compliance obligations.



Cloud Security

Discover attack paths impacting workloads and summarize cloud CVEs to proactively prevent threats and manage cloud security posture more efficiently.



Incident Response

Quickly analyze and respond to security incidents with AI-driven insights and recommendations.



Threat Hunting

Use natural language search for and isolate advanced threats across the environment.



Security Posture Management

Assess and improve your organization's security posture with actionable insights based on your unique organization.



Security Reporting

Generate comprehensive reports that provide clear visibility into your security landscape, aiding in decision-making, threat assessment, compliance, and management/ Board-level briefs.



Threat Intelligence research

Take advantage of Microsoft's extensive threat intelligence by accessing threat articles and threat actor security data on new and emerging threats, helping your organization to prevent and protect itself from potential harm.

How Copilot works with the Microsoft security stack

In the rapidly evolving landscape of cybersecurity, staying ahead of threats is paramount. Copilot emerges as a cutting-edge ally, harnessing the power of artificial intelligence to bolster your security and IT operations. This innovative tool is designed to enhance efficiency, uncover hidden patterns, fortify defenses, and accelerate incident response times.

Key Benefits

Increased Efficiency

Speed up or automate routine tasks, freeing up valuable time for your security team to focus on strategic initiatives.

Reduces human error

Copilot provides insight that humans might miss or otherwise look past.

Hardened Defenses

"Strengthen your security posture using authoritative methods to help reduce the attack surface and vulnerability to threats.

Expert guidance

Get recommendations for things like the top DLP alerts to focus on today, steps to remediate an incident or measure how vulnerable your organization is against a specific bad actor.

Faster Incident Response

Respond to security incidents with unprecedented speed, minimizing potential damage and recovery time.

Copilot integrates seamlessly with key components of the Microsoft security stack, including:



Microsoft Defender XDR

Enhances threat protection and provides advanced attack analytics.



Microsoft Sentinel

Offers cloud-native SIEM and SOAR capabilities for a comprehensive view of the entire digital estate.



Microsoft Intune

Unifies apps and device management to simplify IT and security operations, protect a hybrid workforce and power better user experiences.



Microsoft Purview

Provides data governance and protection, helping to prevent data leaks and ensure compliance.



Microsoft Entra

Manages identities and access, safeguarding against identity-based threats.



Microsoft Defender Threat Intelligence

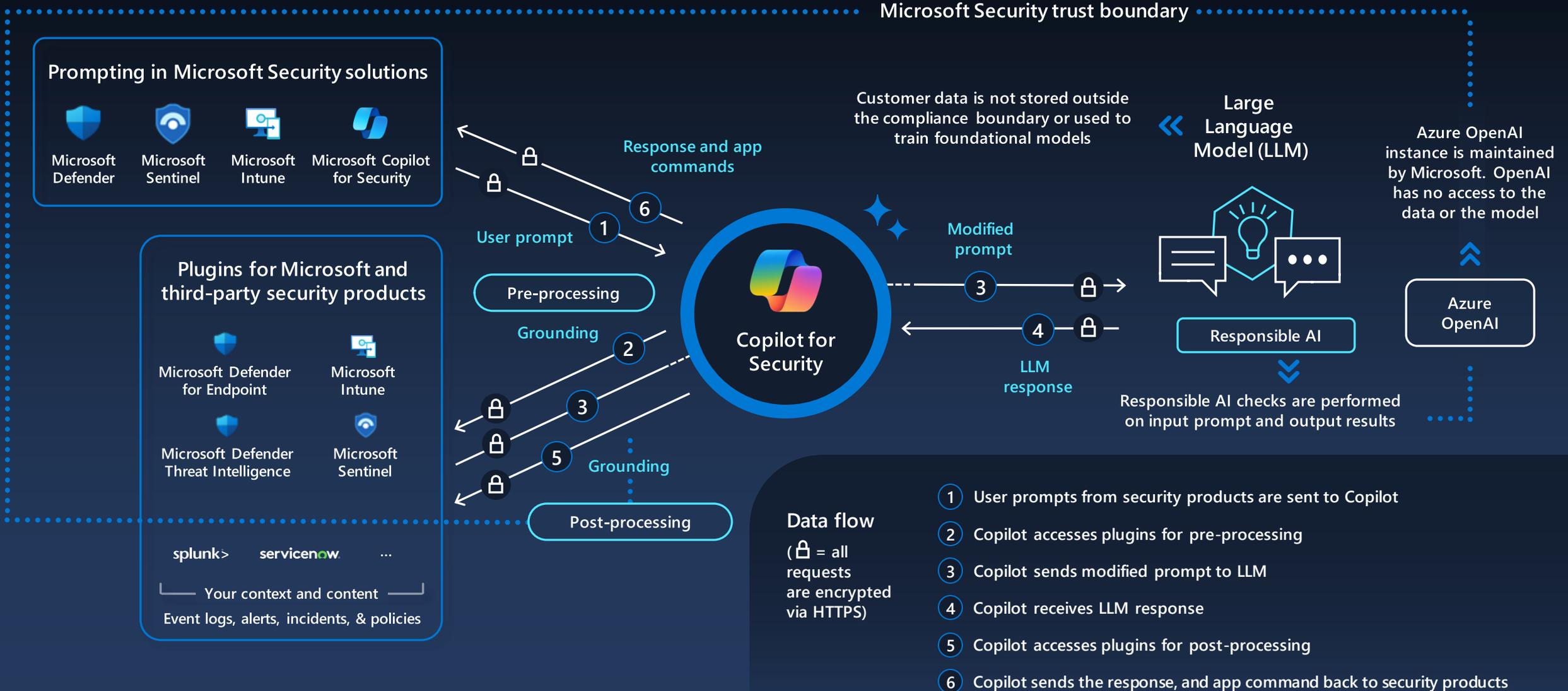
Improves understanding of the threat landscape by providing real-time, context-aware responses to prompts and empowers reactive threat enrichment and proactive hunting scenarios.

The Copilot for Security advantage

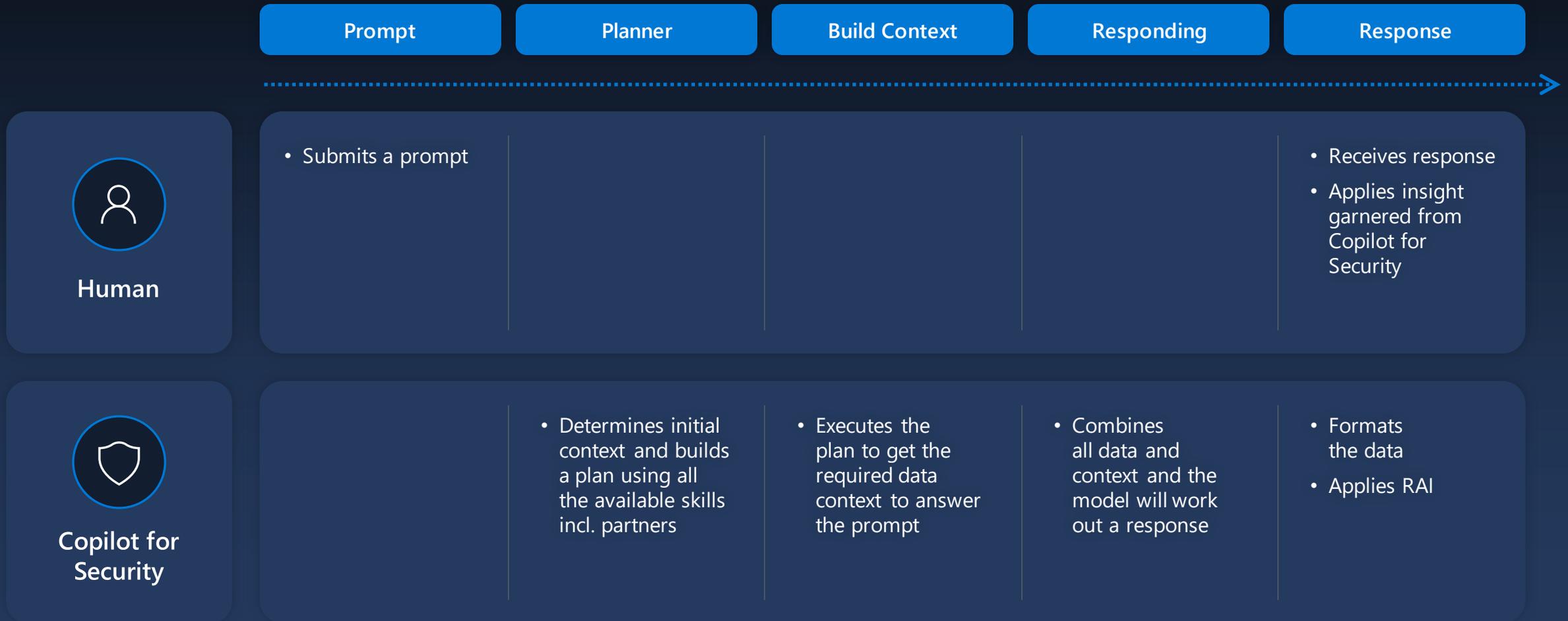
Copilot stitches together information across all security products



Architecture – data flow for Copilot for Security



Architecture – operated with natural language queries



Architecture – example of simple prompts

"Summarize incident 15134 in Microsoft Defender into a paragraph that I can submit to my manager and create a list of entities involved."

"Can you give me information about Pearl Sleet activity, including a list of known indicators of compromise and tools, tactics, and procedures (TTPs)?"

Goal

What is the specific security-related information you need?

"Give me information about incident 18718..."



Context

Why do you need it and how will you use the information?

"...for a report that I can submit to my manager."



Expectations

What format or audience do you want the response tailored to?

"Compile the information in a list, with a short summary."



Source

Is there a plugin, known info, or data source Copilot for Security should use?

"Look in Defender incidents."

[More prompting tips](#)

Architecture – example of simple prompts (cont.)

 How can I improve my security posture?

 Are any of my machines affected?

 Summarize this incident in bullets.

 Which alerts are being triggered the most?

 What is log4shell?

 Tell me about Defender incident 20259.

Tell me about Defender incident 20259.   

>  3 steps completed 25s

Nov 2, 3:14 PM | 26.94s

Defender incident 20259 with Medium severity has a total of 1 alerts. 1 alerts were selected for summarizing the incident.

Some alerts from the incident include:

1. Severity: Medium Start time: 2023-11-02 18:36:24 Description: Unfamiliar sign-in properties relating to attempted sign-in, IP '136.49.226.136' impacting User 'lvandenende'

Here's a short summary of the incident:

The security incident occurred on 2023-11-02 18:36:24 UTC and involved a medium-severity alert. An unfamiliar sign-in attempt was detected, originating from IP address '136.49.226.136' in the United States, impacting user 'lvandenende'. The incident is at the Initial Access stage of the kill chain.

Sources

[Incident Page](#)

 Looks right

 Needs improvement

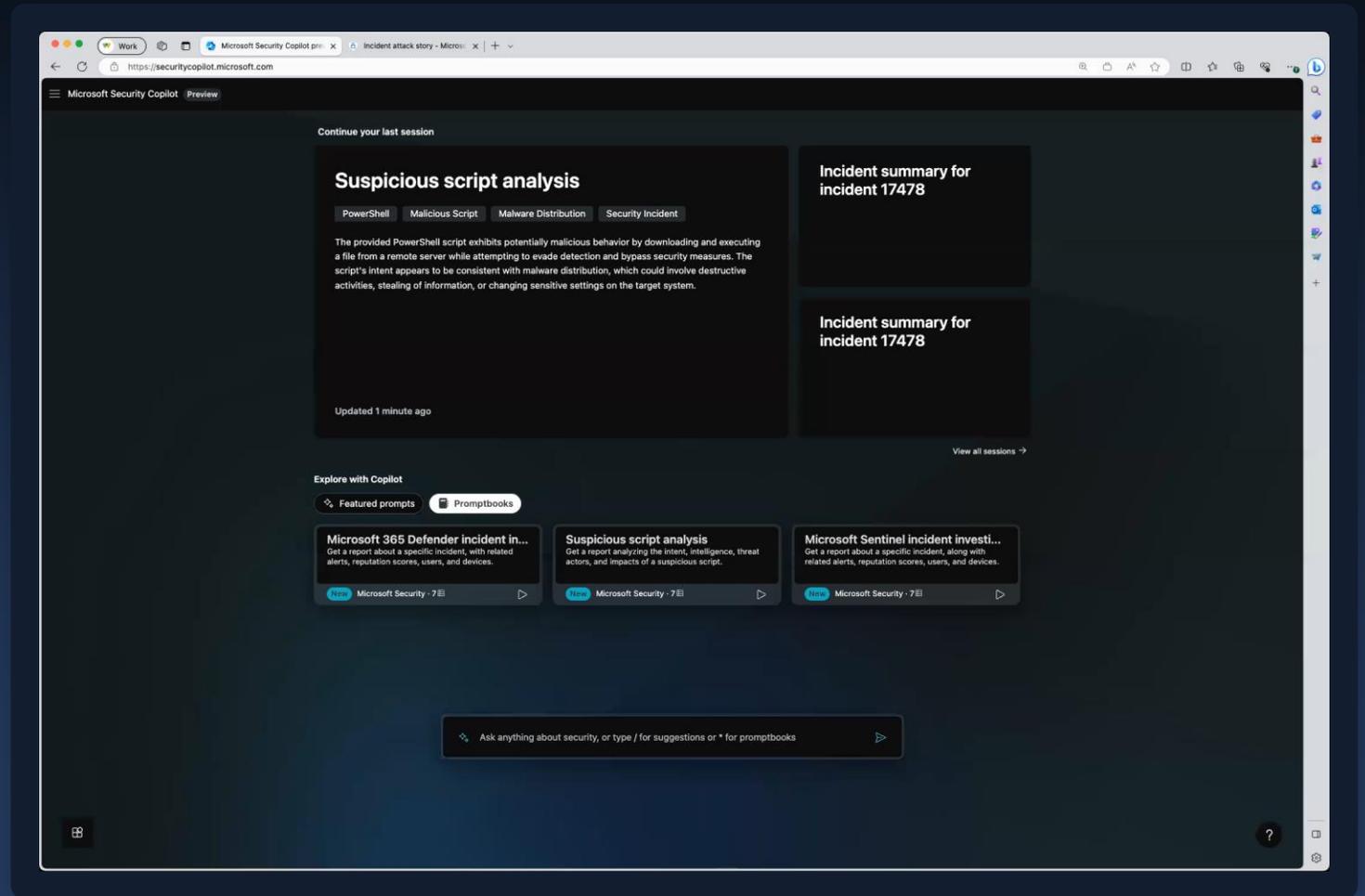
 Inappropriate



Demo – Copilot for Security in action

Watch how Copilot for Security **enriches and summarizes data** from your security tools to **accelerate an investigation.**

Watch the [demo](#)



Maximizing value with Microsoft Security solutions



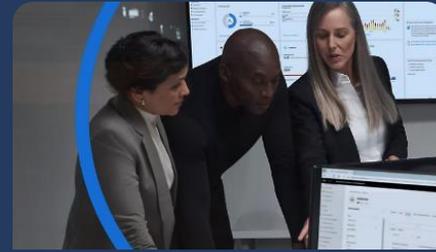
Microsoft Sentinel

Collect security data and correlate alerts from virtually any source with intelligent security analytics.



Microsoft Defender XDR

Prevent and detect cross-domain cyberattacks at the speed of AI. Copilot for Security is now embedded in Microsoft Defender XDR for early access customers.



Microsoft Intune

Mitigate cyberthreats to devices, protect data, and improve compliance across clouds—now embedded with Copilot for Security for early access customers.



Microsoft Defender Threat Intelligence

Understand cyberthreats and expose suspicious infrastructure with dynamic threat intelligence, now included in Copilot for Security at no additional cost.



Microsoft Defender



Microsoft Sentinel



Microsoft Purview



Microsoft Intune



Microsoft Entra

Next steps – Copilot for Security

Partner Readiness

- [Microsoft Learn Documentation](#)
- [Learning Path](#)
- [Copilot for Security Partner Landing Page](#)
- [Microsoft Tech Community Blog](#)
- [Partner Sales & Pre-Sales Enablement Hub](#)
- [Visit our GitHub](#)

Driving Customer Adoption

- Enable services for Plugin use
 - Microsoft Defender XDR
 - Microsoft Sentinel
 - Microsoft Entra
 - Microsoft Intune
 - Microsoft Purview
- Identify Authentication Concerns
 - On Behalf Authentication
 - Privileged Identity Mgmt
 - MDE Device Scope Groups
- Delegated Access Models

Extending Copilot for Security

- Custom plugins and skills
 - [GPT](#)
 - [KQL](#)
 - [API](#)
 - [Logic Apps](#)

•Copilot Plugins

[Azure AI Search \(Preview\)](#)

[Copilot for Security in Microsoft Defender XDR](#)

[Copilot for Security in Entra](#)

[Copilot for Security + Intune](#)

[Copilot for Security and Defender EASM](#)

[Copilot for Security and Defender Threat Intelligence](#)

[Copilot for Security + Purview](#)

The screenshot shows the 'Manage sources' interface for Copilot plugins. It features a search bar and filters for 'All (23)', 'On (8)', and 'Off (15)'. A list of plugins is displayed, each with a toggle switch and a 'Set up' button. The 'Microsoft Defender Threat Intelligence' plugin is highlighted with a red box.

Plugin Name	Description	Status	Action
Microsoft		On	
Azure AI Search (Preview)	Indexed data	On	Set up
Microsoft Defender External Attack Surface Management	Attack surfaces, vulnerable assets, and attack surface insights	Off	Settings
Microsoft Defender Threat Intelligence	Articles, intelligence profiles, vulnerabilities, indicators of compromise, hosts, and threat analytics	On	
Microsoft Defender XDR	Alerts and incidents	On	
Microsoft Entra	Alerts, users, groups, access reviews, and risky services	On	
Microsoft Intune	Devices, apps, policies, and postures	On	
Microsoft Purview	Purview alerts, Insights, and Risk details	On	

Azure AI Search (Preview)

Manage this plugin. [Learn more](#)

Settings ⓘ

↶ Reset

Name of Azure AI Search service ⓘ *

Enter Instance

Name of index ⓘ *

Enter Index

Name of vector field in index ⓘ *

Enter Vector

Name of text field in index ⓘ *

Enter Text

Name of title field in index ⓘ

Enter Title

Value ⓘ *

Enter Value

Copilot for Security in Microsoft Defender XDR

Summarize incidents quickly

BEC financial fraud attack was launched from a compromised account (attack disruption)

Copilot Manage incident Activity log

High Active AlpineSkiHouse - AlpineSkiHouse BEC Fraud Credential Phish Defender Experts Attack Disruption BEC Email threats Alerts

Important! A potentially compromised account was disabled automatically by attack disruption in Microsoft 365 Defender. For more details, select the Assets > Users tab or go to the [Action center](#).

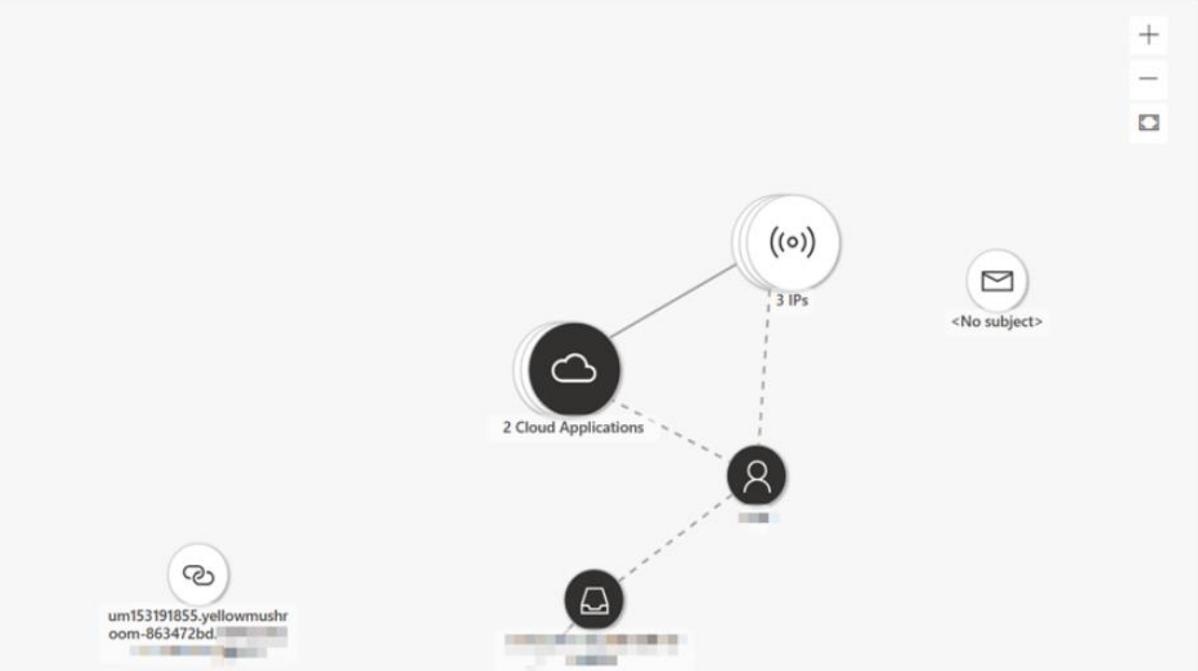
Attack story Alerts (20) Assets (4) Investigations (2) Evidence and Response (25) Recommended actions (21) Summary Similar incidents (0)

Alerts

Play attack story Unpin all Show all

- Mar 15, 2024 2:26 PM Resolved
Activity from a Tor IP address
Name
- Mar 15, 2024 2:26 PM Resolved
Suspicious inbox manipulation rule
Name
- Mar 15, 2024 2:26 PM Resolved
Activity from a Tor IP address
Name
- Mar 15, 2024 2:26 PM Resolved
Suspicious inbox manipulation rule
Name
- Mar 15, 2024 2:34 PM Resolved
A potentially malicious URL click was detected
Name Name
- Mar 15, 2024 2:35 PM Resolved
A potentially malicious URL click was detected

Incident graph Layout Group similar nodes



RELATED THREATS

Threat overview: Cloud identity abuse
22 impacted assets

View threat analytics report

Activity profile: OAuth apps used in BEC and phishing
1 impacted asset

View threat analytics report

View all 3 related threats

Incident details

Assigned to	Incident ID
AlpineSkiHouse - AlpineSkiHouse	2443
Classification	Categories
Not set	Initial access, Defense evasion,

Copilot

Incident summary

Mar 26, 2024 1:58 PM

The high severity BEC financial fraud attack occurred between 2024-03-15 14:26:31 UTC and 2024-03-15 14:40:38 UTC. It was tagged as Attack Disruption, BEC Fraud, and Credential Phish, triggering an automatic Attack Disruption action.

- DefenseEvasion:** The incident began at 2024-03-15 14:26:31 UTC when a suspicious inbox rule was set on the inbox of user 'name'. This rule, named ITCleanup, moved messages to a folder named RSS Feeds. The manipulation involved the IPs 111.111.11.111 and 111.111.11.111 and the cloud apps Microsoft Exchange Online and Microsoft 365. At the same time, 'name' accessed the Tor IP address 111.111.11.111, indicating potential evasion of defenses.
- InitialAccess:** At 2024-03-15 14:34:51 UTC, 'name' clicked on a potentially malicious URL in a mail message titled 'Update'. The URL was 'https://um153191855.yellowmushroom-863472bd...'. Shortly after, at 14:37:02 UTC, an attempted sign-in was detected from the anonymous IP 111.111.11.111.
- CredentialAccess:** At 2024-03-15 14:37:15

Copilot for Security in Microsoft Defender XDR

Take action on incidents through guided responses

BEC financial fraud attack was launched from a compromised account (attack disruption)

High Active AlpineSkiHouse - AlpineSkiHouse BEC Fraud Credential Phish Defender Experts Attack Disruption BEC Email threats Alerts

Important! A potentially compromised account was disabled automatically by attack disruption in Microsoft 365 Defender. For more details, select the Assets > Users tab or go to the [Action center](#).

Attack story Alerts (20) Assets (4) Investigations (2) Evidence and Response (25) Recommended actions (21) Summary Similar incidents (0)

Alerts

- Mar 15, 2024 2:26 PM Resolved Activity from a Tor IP address
- Mar 15, 2024 2:26 PM Resolved Suspicious inbox manipulation rule
- Mar 15, 2024 2:26 PM Resolved Activity from a Tor IP address
- Mar 15, 2024 2:26 PM Resolved Suspicious inbox manipulation rule
- Mar 15, 2024 2:34 PM Resolved A potentially malicious URL click was detected
- Mar 15, 2024 2:35 PM Resolved A potentially malicious URL click was detected
- Mar 15, 2024 2:37 PM Resolved Anonymous IP address
- Mar 15, 2024 2:37 PM Resolved Anonymous IP address
- Mar 15, 2024 2:37 PM Resolved Compromised user account in a recognized attack pattern

Incident graph

Layout Group similar nodes

3 IPs
2 Cloud Applications
Update
um153191855.yellowmushroom-863472bd

RELATED THREATS

Threat overview: Cloud identity abuse
22 impacted assets

View threat analytics report

Activity profile: OAuth apps used in BEC and phishing
1 impacted asset

View threat analytics report

View all 3 related threats

Incident details

Assigned to	AlpineSkiHouse - AlpineSkiHouse	Incident ID	2443
Classification	Not set	Categories	Initial access, Defense evasion, Credential access, Collection
First activity	Mar 15, 2024 2:26:31 PM	Last activity	Mar 15, 2024 2:40:38 PM
Impacted assets			
Users (1)			

Copilot

Incident summary

Mar 26, 2024 1:58 PM

The high severity BEC financial fraud attack occurred between 2024-03-15 14:26:31 UTC and 2024-03-15 14:40:38 UTC. It was tagged as Attack Disruption, BEC Fraud, and Credential Phish, triggering an automatic Attack Disruption action.

- DefenseEvasion:** The incident began at 2024-03-15 14:26:31 UTC when a suspicious inbox rule was set on the inbox of user 'name'. This rule, named ITCleanup, moved messages to a folder named RSS Feeds. The manipulation involved the IPs 111.111.111.111 and 111.111.111.111 and the cloud apps Microsoft Exchange Online and Microsoft 365. At the same time, 'name' accessed the Tor IP address 111.111.111.111, indicating potential evasion of defenses.
- InitialAccess:** At 2024-03-15 14:34:51 UTC, 'name' clicked on a potentially malicious URL in a mail message titled 'Update'. The URL was 'hxxp://um153191855.yellowmushroom-863472bd...'. Shortly after, at 14:37:02 UTC, an attempted sign-in was detected from the anonymous IP 111.111.111.111.
- CredentialAccess:** At 2024-03-15 14:37:15 UTC, 'name' logged on to OfficeHome, indicating a potential compromise of the user account. This activity was associated with the IP 111.111.111.111.
- Collection and DefenseEvasion:** At 2024-03-15 14:39:11 UTC, 'name' performed a New-InboxRule action in Microsoft Exchange Online, indicating a BEC financial fraud attempt. This action was associated with the IP 111.111.111.111. Simultaneously, another suspicious inbox manipulation rule was set, involving the same IP and the cloud app Microsoft Exchange Online.

AI-generated content may be incorrect. Check it for accuracy.

Copilot for Security in Microsoft Defender XDR

BEC financial fraud attack was launched from a compromised account (attack disruption)

High | Active | AlpineSkiHouse - AlpineSkiHouse | BEC Fraud | Credential Phish | Defender Experts | Attack Disruption | BEC | Email threats | Alerts

Important! A potentially compromised account was disabled automatically by attack disruption in Microsoft 365 Defender. For more details, select the Assets > Users tab or go to the [Action center](#).

Attack story | Alerts (20) | Assets (4) | Investigations (2) | Evidence and Response (25) | Recommended actions (21) | Summary | Similar incidents (0)

Alerts

- Mar 15, 2024 2:26 PM Resolved Activity from a Tor IP address
- Mar 15, 2024 2:26 PM Resolved Suspicious inbox manipulation rule
- Mar 15, 2024 2:26 PM Resolved Activity from a Tor IP address
- Mar 15, 2024 2:26 PM Resolved Suspicious inbox manipulation rule
- Mar 15, 2024 2:34 PM Resolved A potentially malicious URL click was detected
- Mar 15, 2024 2:35 PM Resolved A potentially malicious URL click was detected
- Mar 15, 2024 2:37 PM Resolved Anonymous IP address
- Mar 15, 2024 2:37 PM Resolved Anonymous IP address
- Mar 15, 2024 2:37 PM Resolved Compromised user account in a recognized attack pattern
- Mar 15, 2024 2:37 PM Resolved Anonymous IP address

Incident graph

Layout | Group similar nodes

The incident graph illustrates the following relationships:

- 3 IPs (represented by a cloud icon) are associated with 2 Cloud Applications (represented by a cloud icon).
- The 2 Cloud Applications are associated with a user account (represented by a person icon).
- The user account is associated with an email (represented by an envelope icon).
- The email is associated with an update (represented by a document icon).

Legend: — Communication --- Association

RELATED THREATS

Threat overview: Cloud identity abuse
22 impacted assets
[View threat analytics report](#)

Activity profile: OAuth apps used in BEC and phishing
1 impacted asset
[View threat analytics report](#)

[View all 3 related threats](#)

Incident details

Assigned to	AlpineSkiHouse - AlpineSkiHouse	Incident ID	2443
Classification	Not set	Categories	Initial access, Defense evasion, Credential access, Collection
First activity	Mar 15, 2024 2:26:31 PM	Last activity	Mar 15, 2024 2:40:38 PM

Impacted assets

Users (1)	Apps (2)	Application ID	Risk
Name	Microsoft ...	20893	None
	Microsoft ...	11161	None

Copilot

Guided response

Mar 26, 2024 1:59 PM
Completed recommendations 2/4

Status: All

Containment

Completed

- Disable the account Name
Attack Disruption
AI-generated content may be incorrect. Check it for accuracy.

Remediation

New

- Delete similar emails
We found emails that are very similar to emails involved in this incident. Delete these emails to contain the attack.
[Soft delete emails](#) [View similar emails](#)
AI-generated content may be incorrect. Check it for accuracy.
- Completed
- Disable the account Name in AD
AI-generated content may be incorrect. Check it for accuracy.
- New
- Reset password for Name
The user account Name might be compromised. Require the user to change their password on their next sign-in.
[Force password reset](#) [View user](#)

Copilot for Security in Microsoft Defender XDR

Run script analysis with ease

Multi staged attack leading to Domain Controller compromise - Possible Midnight Blizzard (NOBELIUM)

High Active AlpineSkiHouse - AlpineSkiHouse Credential Phish Defender Experts MidnightBlizzard AlpineSkiHouse Microsoft Defender for Endpoint

Attack story Alerts (24) Assets (9) Investigations (3) Evidence and Response (46) Recommended actions (20) Summary Similar incidents (1)

Alerts Incident graph Layout Group similar nodes

Play attack story Unpin all Show all

- Feb 16, 2024 6:17 AM Resolved Suspicious sequence of exploration activities
- Feb 16, 2024 6:18 AM Resolved ADFS private key extraction attempt
- Feb 16, 2024 6:18 AM Resolved Suspected AD FS DKM key read
- Feb 16, 2024 6:18 AM Resolved Suspected AD FS DKM key read
- Feb 16, 2024 6:18 AM Resolved Attempt to hide use of dual-purpose tool
- Feb 16, 2024 6:18 AM Resolved Sensitive credential memory read
- Feb 16, 2024 6:21 AM Resolved Activity from a Tor IP address

Communication Association

Ongoing hands-on-keyboard attack via lm...

6:17:23 AM 2zimba4i.lul.exe executed a script

6:17:23 AM 2zimba4i.lul.exe executed a script

Analyze

```
## Global Variables ##  
$jobId = [guid]:NewGuid()  
$scriptLogPath = 'C:\temp\simulandExecution.log'
```

Content SHA256 f4a490d03f56ab0755613b2cb78f34a0618386f37c65aefc43df2bf0949dbb0d

6:17:23 AM [892] whoami.exe

Suspicious sequence of exploration activities Low Detected Resolved (True positive)

6:17:23 AM 2zimba4i.lul.exe performed system owner/user discovery by invoking whoami.exe

Back to incident details

Ongoing hands-on-keyboard attack via Impacket toolkit High Detected Resolved

AlpineSkiHouse Microsoft Defender for Endpoint

Open alert page Manage alert

Details Recommendations

RECOMMENDATIONS

Remediation & prevention actions you should take

See recommended actions based on your alert classification

View all recommendations

Alert state

Classification True positive Assigned to API-App:API Action

Set Classification

Script analysis Mar 26, 2024 3:10 PM

The provided PowerShell script performs several actions related to logging, exporting the ADFS token signing certificate, and uploading the exported certificate to a remote storage location. The script generates a unique job ID and sets up logging to a local file C:\temp\simulandExecution.log and a remote endpoint http://randomendpoint.com?api-version=2016-10-01&sp=K2FtriggersN2FmanualN2Frun&sv=1.0&sig=*****. It defines a function to add log entries to the local log file and the remote log endpoint. The script exports the ADFS token signing certificate and saves it to a local file C:\ProgramData\ADFS\TokenSigningCertificate.pfx. Finally, the script uploads the exported ADFS token signing certificate to a remote storage location https://randomcollector.com.

- The script generates a unique job ID and sets up logging to a local file and a remote endpoint. Show code
- The script defines a function to add log entries to the local log file and the remote log endpoint. Show code
- The script exports the ADFS token signing certificate and saves it to a local file. Show code
- The script uploads the exported ADFS token signing certificate to a remote storage location. Show code

AI-generated content may be incorrect. Check it for accuracy.

Copilot for Security in Microsoft Defender XDR

Generate device summaries

The screenshot displays the Microsoft Defender XDR interface for a device named "Windows device1". The interface is divided into several sections:

- Overview:** Shows the device's risk level as **High** and exposure level as **Medium**. It also indicates that 2 users are logged on.
- Active alerts (Last 180 days):** Shows 26 active alerts and 6 active incidents. A bar chart indicates 3 High, 14 Medium, and 1 Low severity alerts.
- Security assessments:** Shows 57 active security recommendations and 38 discovered vulnerabilities (30 High, 8 Medium).
- Logged on users (Last 30 days):** Shows 2 logged on users.
- Device health status:** A table showing the status of various components:

Type	State	Date & time
Last full scan	No scan performed	
Last quick scan	Completed	Mar 26, 2024 4:44:41 AM
Security intelligence	Version 1.407.714.0	Mar 25, 2024 8:01:03 PM
Engine	Version 1.1.24020.9	Mar 25, 2024 8:01:03 PM
Platform	Version 4.18.24010.12	Feb 28, 2024 12:43:47 AM
Defender Antivirus mode	Active	Mar 26, 2024 5:15:06 PM
- VM details:** A sidebar on the left provides details about the device, including its category (Endpoint), subtype (Workstation), OS (Windows 10 64-bit), and health state (Active).
- Copilot summary:** A panel on the right provides a summary of the device's security state, generated by Copilot. It highlights that the device is non-compliant due to an outdated platform and a high severity vulnerability.

Copilot for Security in Microsoft Defender XDR

Analyze files promptly

Search > Files > rubeus.exe

rubeus.exe

Signer: ▲ Unsigned • Size: 429.06 KB

File was submitted for Deep analysis. Status: Success. See report

Overview Incidents & Alerts Observed in organization File names File content Deep Analysis

File Details

Object details

SHA1
fc870d086c53ded2e94300f7569aa9478186f2c7

SHA256
a1fdd460edd35ed449d32cc43bc15675c48a314a6fa5fb158e3bc4fea460be1

MD5
7a7c8fa61d748cbe0034846015e5bd8a

File size
429.06 KB

Is PE
true

Signer
Unsigned file
This file's signer is unknown

File Capabilities (5 techniques)

Attack technique	Tactics	De
T1132.001: Standard Enc...	Command and Control	Th
T1001.002: Steganograp...	Command and Control	Th
T1033: System Owner/U...	Discovery	Th

View all (5 techniques)

PE metadata

Incidents & Alerts

11 active alerts, 2 incide...

High (4) Medium (3) Low (2) 1 more

View Incidents & Alerts

Observed devices (last 30 Days)

1 device

Date (First / Last)	Devices
Mar 25, 2024 (First)	parkcity-win10v...

View all devices

Observed on cloud apps (last 30 days)

Worldwide observed devices

Medium prevalence
345

First seen	Last seen
Jun 29, 2022	Mar 13, 2024

VirusTotal

54/69 (High risk)

View in VirusTotal

File names

File name	Number of devices
rubeus.exe	1
Rubeus.exe	1

View all file names

Copilot

File analysis
Mar 27, 2024 9:35 AM

Overview

The file has been detected as malicious by 54 out of 69 engines in the VirusTotal static scan, including the Microsoft engine which labeled it as VirTool:Win32/Kekeo.AIMTB. This high detection ratio is a significant risk indicator. The file lacks digital certificate information, which could suggest potential risks. The malware detection tool has determined the file as malware. The size of the image in the PE metadata is 458752. These findings suggest potential security threats associated with the file.

Hide details

Strings

The provided strings reveal several potential areas of interest in the file's behavior. The presence of "SendBytes", "ProxyFileInfo32", and "GetHostName" could suggest network-related activities, possibly indicating data exfiltration or command and control communication. The string "ImpersonateLoggedOnUser" is particularly noteworthy, as it may imply attempts to escalate privileges or perform actions under the guise of a legitimate user. The strings "ERROR_NO_NETWORK" and "ERROR_BUSY_DRIVE" could be indicative of error handling routines, which might be used to evade detection or maintain persistence in the event of a failure. The presence of "LocalMachine" and "hToken" might suggest attempts to interact with system-level objects or settings, potentially indicating a broader scope of malicious activity.

The string "25E3E48132FBDBE9B7C0C6C54D7C10A5DE12A105AA3E5DE2A0DC808F24587A5" appears to be a hash value, which could be used for a variety of purposes, such as verifying the integrity of data, identifying unique data, or as part of a cryptographic process.

The presence of "RPC_DISPATCH_TABLE", "_RPC_SID", and "NdrParserFlags" could suggest the use of Remote Procedure Call (RPC) technology, which might be used for inter-process or network communication.

The strings "set_ServerCertificateValidationCallback", "set_cusec", "set_CredentialInfo", and "set_value" could be indicative of attempts to manipulate or interact with security-sensitive data or settings.

The absence of obviously malicious strings does not necessarily mean the file is benign. It could be the case that the file did not have strings, or the strings were not captured by the analysis, or the strings are obfuscated. Therefore, further analysis is recommended.

API calls

The file imports _CorExeMain from mscoree.dll, suggesting it's a .NET file that initializes the CLR and loads the .NET application.

Certificates

The absence of digital certificate data for this file is noteworthy. This lack of information could potentially indicate unknown risks and warrants further investigation to ascertain the file's authenticity and security.

AI-generated content may be incorrect. Check it for accuracy.

Copilot for Security in Microsoft Defender XDR

Write incident reports efficiently

Incidents > Human-operated ransomware attack was launched from a compromised asset (attack disruption)

Human-operated ransomware attack was launched from a compromised asse...

High Resolved AlpineSkiHouse - AlpineSkiHouse Ransomware Attack Disruption New Device HumOR Email threats Alerts AlpineSkiHouse

Important! Attack disruption has automatically taken multiple response actions. For more details, go to the [Action center](#).

Attack story Alerts (33) Assets (7) Investigations (5) Evidence and Response (49) Summary Similar incidents (0)

Alerts

Play attack story Unpin all Show all

- Mar 21, 2024 7:05 PM Resolved
Potential human-operated malicious activity
WindowsDevice3.domain.com 3 Users
- Mar 21, 2024 7:06 PM Resolved
Potential human-operated malicious activity
WindowsDevice4.domain.com 2 Users
- Mar 21, 2024 7:40 PM Resolved
Potential human-operated malicious activity
WindowsDevice4.domain.com
- Mar 21, 2024 7:59 PM Resolved
Possible lateral movement
WindowsServer1
- Mar 21, 2024 7:59 PM Resolved
Suspicious remote activity
WindowsDevice3.domain.com 2 Users
- Mar 21, 2024 7:59 PM Resolved
Suspicious remote activity
WindowsDevice4.domain.com 2 Users
- Mar 21, 2024 7:59 PM Resolved
System recovery setting tampering
WindowsDevice4.domain.com Account name

Incident graph

Layout Group similar nodes

Communication Association

RELATED THREATS

Threat overview: Human-operated ransomware
36 impacted assets
[View threat analytics report](#)

Activity profile: Manatee Tempest – from FakeUpdates to ransomware
13 impacted assets
[View threat analytics report](#)

Incident details

Assigned to	AlpineSkiHouse - AlpineSkiHouse	Incident ID	21239
Classification	True alert	Categories	Execution, Credential access, Lateral movement, Ransomware, Suspicious activity
First activity	Mar 21, 2024 7:05:32 PM	Last activity	Mar 21, 2024 8:16:16 PM

Incident report

Mar 31, 2024 4:10 PM

Incident title
Human-operated ransomware attack was launched from a compromised asset (attack disruption)

Incident details

Analysts AlpineSkiHouse - AlpineSkiH... Analyst@domain.com

Time created 03/21/2024 19:05:32
First log 03/21/2024 20:11:33
Last log 03/31/2024 13:28:30
Time closed 03/31/2024 12:43:22

Incident summary
The high severity incident 'Human-operated ransomware attack was launched from a compromised asset' occurred between 2023-03-21 19:05:32 UTC and 2023-03-21 20:16:16 UTC. It was tagged as Attack Disruption and Ransomware, triggering an automatic Attack Disruption action.

- The incident began at 2023-03-21 19:05:32 UTC with potential human-operated malicious activity on the device 'Device1' (Windows10). The activity involved 7 files, including 'subtler.doc' and 'subtler.doc.lockbit', 2 IPs 11.111.11.111 and 111.222.33.444, and 9 processes, including 'powershell.exe' (running as SYSTEM), impacting users 'Account name 1' and 'Account name 2'.
- At 2023-03-21 19:06:42 UTC, similar malicious activity was detected on the device 'Device2' (Windows10), involving 3 files, including 'nontrigonometrical.pdf.lockbit', and 6 processes, including 'vssadmin.exe'.
- LateralMovement:** At 2023-03-21 19:59:54 UTC, possible lateral movement was detected relating to IP 111.222.33.444, impacting the device 'WindowsServer1' (WindowsServer2016). This was followed by suspicious remote activity on 'Device1' and 'Device2', involving processes such as 'bcdedit.exe' and 'powershell.exe', and impacting user 'Account name 1'.
- At 2023-03-21 19:59:56 UTC, system recovery setting tampering was detected on both 'Device2' and 'Device1', involving processes such as 'vssadmin.exe' and 'WmiPrvSE.exe' (running as NETWORK SERVICE), and impacting user 'Account name 1'.
- Execution:** At 2023-03-21 19:59:56 UTC, suspicious WMI process creation was detected on both 'Device2'

Copilot for Security in Microsoft Defender XDR

Hunt like a pro

Advanced hunting

[New query](#) +

Schema Functions ...

Search

Alerts & behaviors

- AlertEvidence
- AlertInfo
- BehaviorEntities
- BehaviorInfo

Apps & identities

- AADSignInEventsBeta
- AADSpnSignInEventsB...
- CloudAppEvents
- IdentityDirectoryEvents
- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents

Email & collaboration

- EmailAttachmentInfo
- EmailEvents
- EmailPostDeliveryEve...
- EmailUrlInfo
- UrlClickEvents

Run query Last 7 days Save Share link Copilot Manage rules

Query

1

Getting started Results Query history

0 items

Search

Customize columns

Time ↓

Query

Query time

State

No data available

Copilot

Mar 26, 2024 4:20 PM

Give me all the devices that signed in within the last hour

Mar 26, 2024 4:21 PM

The Kusto Query Language (KQL) query to retrieve all devices that signed in within the last hour is as follows:

```
AADSignInEventsBeta  
| where Timestamp > ago(1h)  
| project DeviceName
```

Run query

AI-generated content may be incorrect. Check it for accuracy.

Ask a question to generate a query

Copilot for Security in Microsoft Defender XDR

Monitor threat intelligence

- Home
- Exposure management
- Investigation & response
- Threat intelligence
 - Threat analytics
 - Intel profiles
 - Intel explorer
 - Intel projects
- Assets
- Microsoft Sentinel
- Identities
- Endpoints
- Email & collaboration
- Cloud apps
- SOC optimization
- Reports
- Learning hub
- Trials
- More resources
- System
- Customize navigation

Threat analytics

Copilot Email notification settings Help resources

Threat intel reports are being updated in stages to align with the Microsoft 365 Defender rebrand into Microsoft Defender XDR.

Ransomware 96 Extortion 0 Phishing 58 Hands on keyboard 0 Activity group 178 Vulnerability 108 Attack campaign 0 Tool or technique 0

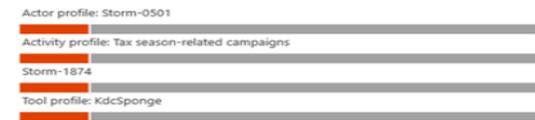
Latest threats



High-impact threats



Highest exposure threats



Search

387 items Customize columns Filter

Threat	Alerts	Impacted assets	Threat exposure level	Misconfigured devices	Vulnerable devices	Report type	Published	Last updated
Actor profile: Storm-0501	0 active / 0		13 - Low	63	Not available	Activity groups	Mar 20, 2024 7:05 PM	Mar 20, 2024 7:05 PM
Activity profile: Tax season-relat...	0 active / 0		13 - Low	63	Not available	Attack campaigns	Mar 19, 2024 11:13 PM	Mar 19, 2024 11:13 PM
Activity profile: Mango Sandsto...	0 active / 0		0 - Low	1	Not available	Attack campaigns	Mar 18, 2024 5:45 PM	Mar 18, 2024 5:45 PM
Technique Profile: Bring your o...	0 active / 0		0 - Low	63	0	Tools & techniques	Mar 18, 2024 4:00 PM	Mar 18, 2024 4:00 PM
Vulnerability profile: CVE-2024-...	0 active / 0		0 - Low	61	0	Vulnerabilities	Mar 13, 2024 3:00 PM	Mar 13, 2024 3:00 PM
Storm-1874	0 active / 0		13 - Low	63	Not available	Activity groups	Mar 7, 2024 6:19 PM	Mar 7, 2024 6:19 PM
Vulnerability profile: Mirth Con...	0 active / 0		0 - Low	63	0	Vulnerabilities	Mar 1, 2024 12:28 PM	Mar 1, 2024 12:28 PM
Vulnerability profile: CVE-2024-...	0 active / 0		0 - Low	63	0	Vulnerabilities	Feb 26, 2024 1:09 PM	Feb 26, 2024 1:09 PM
Vulnerability profile: Multiple v...	0 active / 0		0 - Low	63	0	Vulnerabilities	Feb 7, 2024 4:46 PM	Feb 14, 2024 2:38 PM
Vulnerability profile: CVE-2024-...	0 active / 0		2 - Low	63	10	Vulnerabilities	Feb 13, 2024 10:20 AM	Feb 13, 2024 10:20 AM

Copilot

Try these prompts to start working with Copilot to prioritize and get relevant threat intelligence.

- Summarize**
Give me an overview of the latest threats to my organization.
- Prioritize**
Which threats should I focus on based on their exposure scores?
- Ask**
Which threat actors are targeting the communications infrastructure?

Ask about actors, attack techniques, and other threat intelligence

Copilot for Security Entra

Risky User Details

Reset password Confirm user compromised Dismiss user risk Block user | User's risk detections ...

Summarize

Basic info

Recent risky sign-ins

Detections not linked to a sign-in

Risk history

Summary by Copilot (Preview)

Generated by Copilot

- User Giovanna Costa has one recent risky activity with High risk.
- The risk detection type is Microsoft Entra threat intelligence.
- Microsoft Entra threat intelligence indicates user activity that is unusual for the user or consistent with known attack patterns. This detection is based on Microsoft's internal and external threat intelligence sources.
- Risky sign-in 1 (RequestId: 81e5c594-d704-497c-9e4a-..., CorrelationId: 34a26cec-6930-4ce5-9bd9-...) with High risk level occurred on 2024-03-26T22:59:48 UTC for Resource Azure Portal. The sign-in IP was ... and location was Redmond, Washington US. The IP, ASN, Location, Browser Id and Device Id and were unfamiliar to the user. There was no MFA for this sign-in.

AI-generated content may be incorrect

What to do

Check to ensure this user is in scope of these risk-based Conditional Access policies which will shorten the time to mitigate the attack, automatically close the risk, and save you time and effort.

If you do not have those policies:

1. [Create a sign-in risk based policy](#)
2. [Create a user risk based policy](#)

For now, investigate this user for indicators of compromise and take action using the buttons above. Use our playbooks below for step-by-step guidance.

Help and documentation

[What is risk in ID Protection?](#)

[Incident Response Playbooks](#)

[Risk-based Access Policies](#)

Copilot for Security Intune



Intune

Devices, privileges, policies, and postures



- How many users is ContosoApp assigned to?
- Which groups are ContosoApp assigned to?
- How many apps are assigned to the device ID *Enter the device ID* in Intune?
- Why is "Allow Microsoft Store App to auto update" policy applying to DeviceA?
- Tell me about Intune devices for user UserA.
- Why is PolicyA applying on DeviceB?

- What apps are added to Intune?
- What Intune apps are assigned the most?
- How many devices were enrolled in Intune in the last 24 hours?
- Tell me about Intune devices for Jon Smith.

Connect Copilot to Defender EASM

woodgroveMDEASM ☆ ... ✕

Microsoft Defender EASM

🗑️ Delete resource ℹ️ Learn

^ Essentials JSON View

Resource group : [Woodgrove-RG](#)

Location : East US

Subscription : [Woodgrove - GTP Demos \(External/Sponsored\)](#)

Subscription ID :

← **Microsoft Defender External Attack Surface Management settings** ✕

Manage this plugin. [Learn more](#)

Settings ⌵

Resource name ⌵

Subscription ID ⌵

Resource group name ⌵

Cancel Save

Copilot for Security and Defender Threat Intelligence

- Show me the reputation of the host *<host name>*.
- Get resolutions for IP address *<IP address>*.

- Tell me more about Silk Typhoon.
- Share the IOCs associated with Silk Typhoon.
- Share the TTPs associated with Silk Typhoon.
- Share threat actors associated with Russia.

- Share the technologies that are susceptible to the vulnerability CVE-2021-44228.
- Summarize the vulnerability CVE-2021-44228.
- Show me the latest CVEs.
- Show me threat actors associated with CVE-2021-44228.
- Show me the threat articles associated with CVE-2021-44228.

Copilot for Security + Purview

- *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.*