

Microsoft Copilot for Security

Shruti Ailani
Chris van Uden

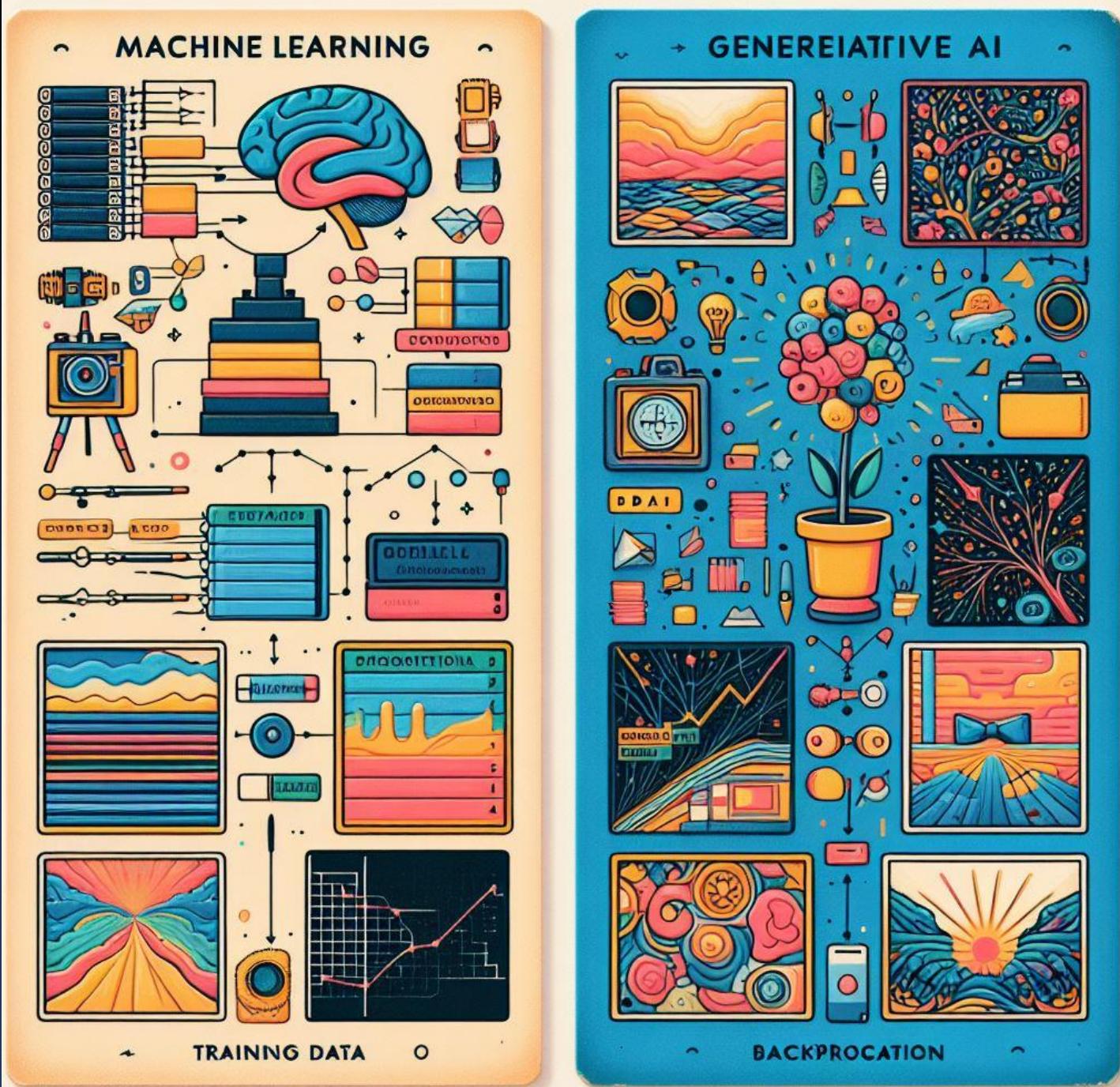
April 04 2024



Welcome!



AI and Large Language Models (LLMs)



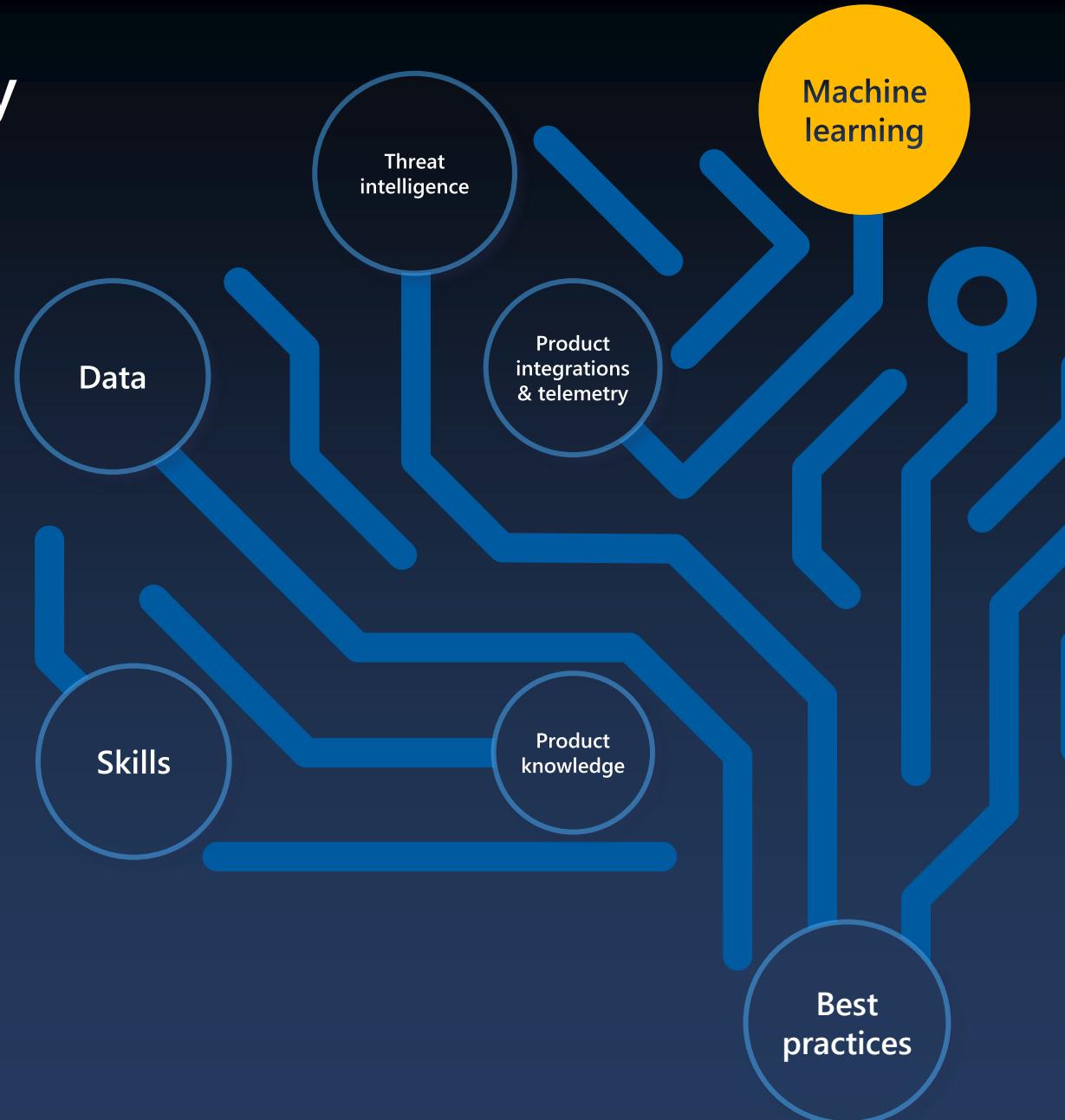
Spot the similarity!

- Product for the masses
- Affordable cost
- Revolutionizing tech



Microsoft Copilot for Security

- **Hear from the Brains behind Copilot for Security**
- **How does it work**
- **Customer experiences**
- **What's beyond the tip of the iceberg**
- **Q&A**

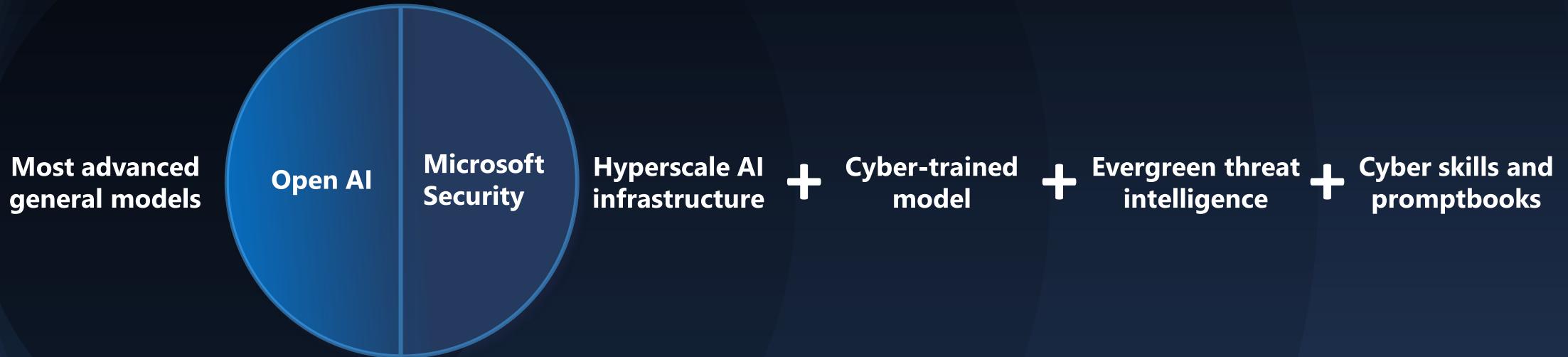


Hear from the Brains behind Copilot for Security



Nick Goodman

The Microsoft Security Copilot advantage



- Multiple copilots; here's the Security Copilot
- It's not ChatGPT



Microsoft Copilot for Security

Defending at machine speed

"It takes us three minutes to do a task that used to take at least a few hours"

- Private preview customer



Enable **response** in minutes,
not hours



Simplify the **complex** with natural language prompts and easy reporting



Catch what others miss with deeper understanding of your enterprise



Upskill your **security talent** with cyber-trained generative AI

Primary use cases



Incident summarization



Impact analysis



Reverse engineering of scripts



Guided response

Experiences to meet you where and how you work

Standalone

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

The screenshot shows the Microsoft Security Copilot interface. At the top, it says "Continue your last session". Below are three cards:

- Tell me about Defender incident 20259.**

The customer inquired about the Defender incident 20259 with Medium severity. The incident involved a medium-severity alert for an unfamiliar sign-in attempt from IP address 136.49.226.136 in the United States. The incident was detected on 2023-11-02 18:36:24 UTC and involved an user named 'Vandenende'. The incident was at the Initial Access stage of the kill chain. The user was affected by the attempted sign-in and the incident is still ongoing. The incident was reported to the customer by the agent. The customer was asked to provide a summary of the incident. The agent provided a summary of the security incident.
- Tell me more about Cobalt Strike.**

Cobalt Strike is a penetration testing and adversary emulation framework that was first released in 2012. It was initially designed to...
- Tell me about my latest incidents.**

These include unfamiliar sign-in properties, multiple failed user-logon attempts, threat intelligence session, attack using AITM...

At the bottom, there's a "View all sessions" button and a "Explore with Copilot" section with "Featured prompts" like "Threat actor profile", "Vulnerability impact assessment", and "Microsoft Sentinel incident investigation". There's also a search bar at the bottom.

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.

The screenshot shows the Microsoft Purview Insider Risk Management interface. On the left, there's a navigation menu with "Insider Risk Management" selected. In the center, there's a card for an alert titled "(7bbc3040) Data theft by departing users".

Activity that generated this alert: EpiphanyCopilotToRemoteDesktopSession
87/100 High severity | Sept 28, 2023 (UTC)
45 events: File copied through remote desktop session
24 events: File containing personal info, including: Credit Card Number

Triggering event: Sept 26, 2023 (UTC)
An HR connector imported a resignation date for this user.

User details: jdoe@edsocf.onmicrosoft.com
View all details

User alert history: Last 30 days
Data theft for departing users
Sensitive file access
Security violation
View all alert history

Alert summary: October 1, 2023 2:41 PM
The alert with ID 7bbc3040 is a high severity Insider Risk Management alert involving user Jane Doe (jdoe@edsocf.onmicrosoft.com) that was detected on September 30, 2023. The policy "Data theft for departing users" was triggered when the HR connector imported a resignation date for this user on September 26, 2023. The user was involved in a sensitive file access event where sensitive info were copied to a remote desktop session related to this alert getting generated. This alert has a high risk and has 5 alerts and 1 case associated with them. This alert is in a confirmed state and is being investigated by Bob Dylan. The alert also has a case "DepartingUser_Investigation" associated with it.

At the bottom, there's a "Natural language prompt" input field and a "Generate KQL" button.

Under NDA only

Microsoft's End-to-End Security



Under NDA only

Copilot for Security powering Microsoft Defender



Security Posture
Management



Incident Investigation
and Response



Security Reporting

TI-driven risk assessment

Incident Summary

Incident Guided Response

NL Query Assistant

Script Analyzer

Analyst Activity Report

Boost SOC efficiency

Upskill your analysts

Copilot for Security powering Microsoft Defender



Security Posture
Management



Incident Investigation
and Response



Security Reporting

AI-driven risk assessment

Incident Summary
Device Summary
Incident Guided Response
NL Query Assistant
Script Analyzer
File Analyzer
Analyst-enduser communication

Analyst Activity Report
PDF Report Export

Boost SOC efficiency

Upskill your analysts



Can you summarize sentinel incident 29088 contained in workspace woodgrove-loganalyticsworkspace?

> 3 steps completed 1 min



2:09 PM

Incident 29088 in the Woodgrove-LogAnalyticsWorkspace has the title "SAP - (Preview) File Downloaded From a Malicious IP Address" and is described as a user downloading a file from an SAP system using an IP address known to be malicious. The incident has a severity of "High" and is currently in "New" status. The incident was first detected on 2023-06-21T18:38:41.103Z and last updated on 2023-06-22T18:43:44.4744196Z.

The incident has 1 associated alert with the same title and description. The alert was generated on 2023-06-22T18:43:44.1397144Z and has a tactic of "Exfiltration".

There are 3 entities associated with this incident:

1. IP: 185.82.217.3
2. Host: CPC-mscot-S0C0S (Windows, FQDN: cpc-mscot-s0c0s)
3. Account: [mscott@woodgrove.ms](#) (AzureAD domain, DisplayName: [mscott@woodgrove.ms](#))

Please note that this is a summary of the available information, and further investigation may be required to fully understand the incident.



Confirm



Off-target



Report



Pin

Ask anything about security, or type / for suggestions



Confirm Off-target Report

You note the IP address is malicious, can you provide the reputation and more details about why it's malicious?

> 3 steps completed 1 min

2:13 PM

The IP address 185.82.217.3 has a reputation score of 100, which classifies it as malicious. The following rules contribute to its malicious classification:

1. Cyber Threat Intelligence - Cobalt Strike

- Description: Cobalt Strike
- Severity: 5
- Link: [Cobalt Strike](#)

2. Cyber Threat Intelligence - Silk Typhoon

- Description: Silk Typhoon
- Severity: 5
- Link: [Silk Typhoon](#)

3. ASN

- Description: Infrastructure hosted by this ASN frequently exhibits suspicious behavior
- Severity: 4
- Link: None

These rules indicate that the IP address is associated with known cyber threat intelligence profiles and suspicious behavior.

Confirm Off-target Report



Ask anything about security, or type / for suggestions

Severity: Link: None

These rules indicate that the IP address is associated with known cyber threat intelligence profiles and suspicious behavior.

Confirm Off-target Report Pin

Tell me more about cobalt strike and silk typhoon.

> 3 steps completed 1 min +2

2:14 PM

Here's more information about Cobalt Strike and Silk Typhoon:

1. Cobalt Strike
Cobalt Strike is a commercial, full-featured penetration testing tool that allows an attacker to deploy an agent named "Beacon" on the victim's machine. Beacon includes a wealth of functionality to the attacker, including command execution, keylogging, file transfer, SOCKS proxying, privilege escalation, and more. It is often used by advanced persistent threat (APT) groups and cybercriminals for post-exploitation activities. Cobalt Strike has been observed in various cyber attacks, including those taking advantage of the Exchange Server vulnerabilities. You can read more about it in this [article](#).

2. Silk Typhoon (HAFNIUM)
Silk Typhoon is a threat actor group that has been observed exploiting the Exchange Server vulnerabilities. They are known for their sophisticated attacks and have targeted various organizations worldwide. Microsoft researchers have observed a steady increase in signals indicating exploitation by threat actors other than Silk Typhoon. Numerous other attackers have been seen adopting the exploit into their toolkits. You can read more about Silk Typhoon and their activities in this [article](#).

Confirm Off-target Report Pin

Ask anything about security, or type / for suggestions



these devices compliant.

> 3 steps completed 1 min

2:15 PM

Here are the devices associated with the user [mscott@woodgrove.ms](#) and their compliance status:

Device Name	Manufacturer	Model
MSCOTT-SURFACE2	Microsoft Corporation	Surface Laptop 2
DESKTOP-LDLSMJL	Microsoft Corporation	Virtual Machine
CPC-mscot-S0C0S	Microsoft Corporation	Cloud PC Enterprise 2vCPU/8GB/128GB

To make these devices compliant, follow these steps:

- 1. Remain in contact**
Ensure that the devices remain in contact with the Intune service. Devices that do not remain in contact may be considered noncompliant. Check the device's network connectivity and ensure it can communicate with the Intune service.
- 2. Defender for Endpoint - Device Risk**
For the device CPC-mscot-S0C0S, ensure that the required security level for Device Threat Protection is met. This can be achieved by updating the device's security software, applying security patches, and ensuring that the device is protected against known threats.

After addressing these issues, the devices should become compliant. Keep in mind that it may take some time for the compliance status to update in Intune.

Confirm Off-target Report Pin

Ask anything about security, or type / for suggestions





```
1 let userEmails = dynamic(["mscott@woodgrove.ms", "mscott@hipstabank.com"]);
2 union
3 (
4     AlertEvidence
5     | where AccountUpn in (userEmails) or AccountName in (userEmails)
6     | extend UserEmail = iif(isnull(AccountUpn), AccountName, AccountUpn)
7 ),
8 (
9     EmailEvents
10    | where SenderFromAddress in (userEmails) or RecipientEmailAddress in (userEmails)
11    | extend UserEmail = iif(SenderFromAddress in (userEmails), SenderFromAddress,
12      RecipientEmailAddress)
13 )
14 | where Timestamp > datetime("2023-07-12T17:57:34Z") - 30d
15 | project Timestamp, UserEmail, Title, AlertId, NetworkMessageId, EmailDirection
```



I found a total of 15 records, and here's the table with the results:

15 rows x 6 columns

Timestamp	UserEmail	Title
2023-06-21T23:07:31Z	mscott@woodgrove.ms	
2023-06-28T23:36:52Z	mscott@woodgrove.ms	
2023-06-28T22:48:19Z	mscott@woodgrove.ms	
2023-07-06T23:14:39Z	mscott@woodgrove.ms	
2023-06-23T00:00:50Z	mscott@woodgrove.ms	

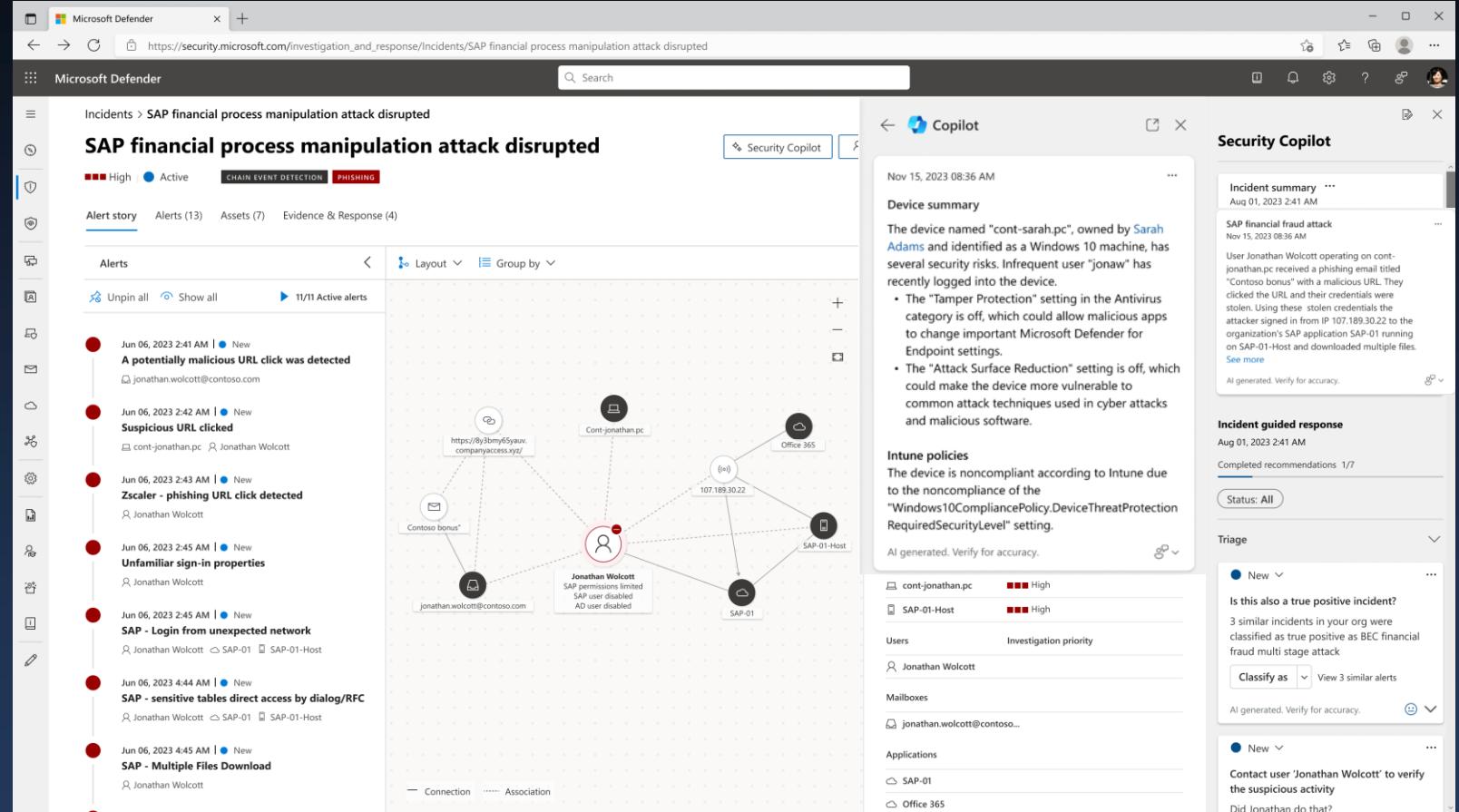
Confirm Off-target Report

Ask anything about security, or type / for suggestions



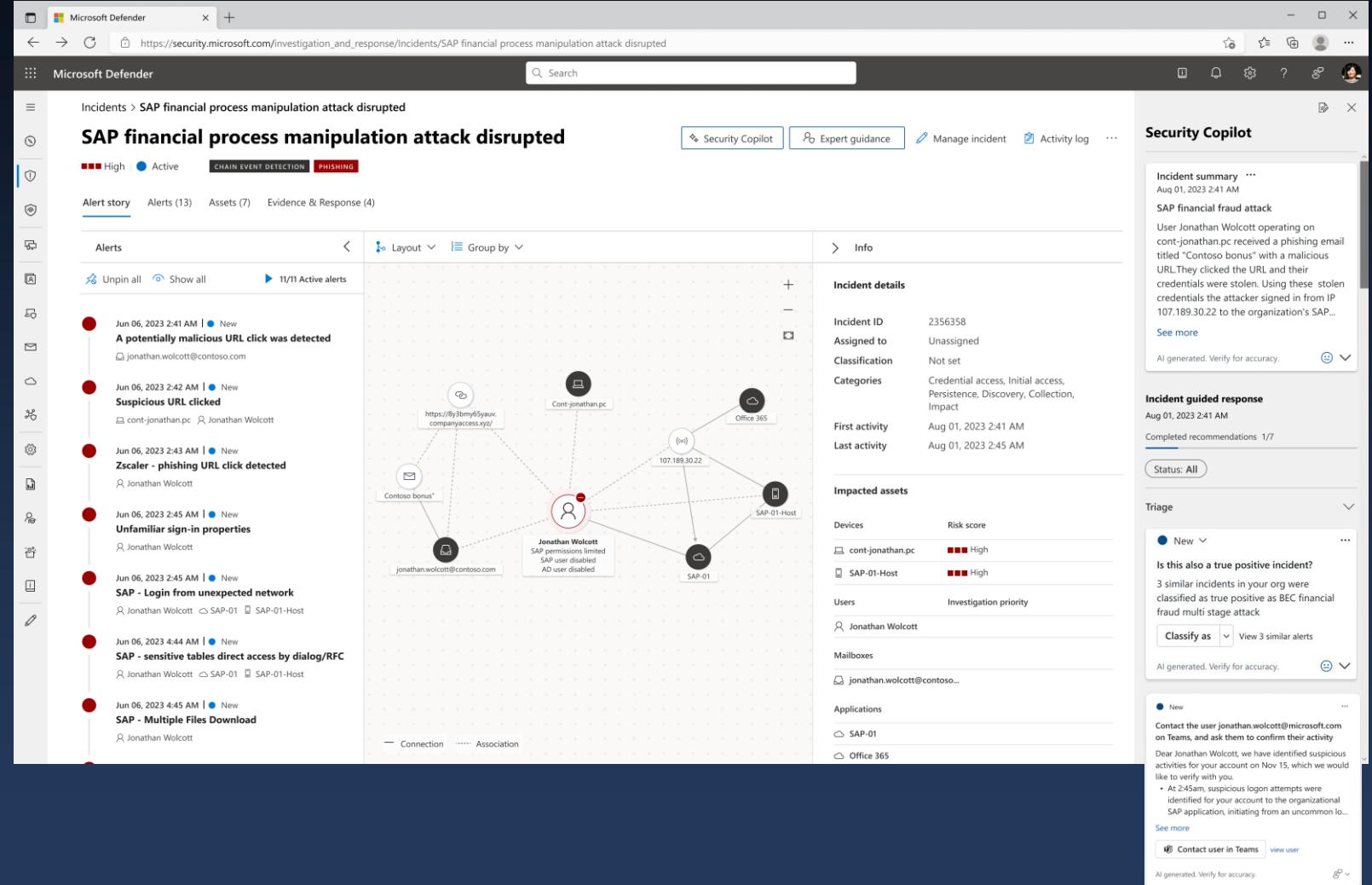
Guided incident investigation & response

- Understand the attack story in seconds with **incident summaries** and **asset summaries**



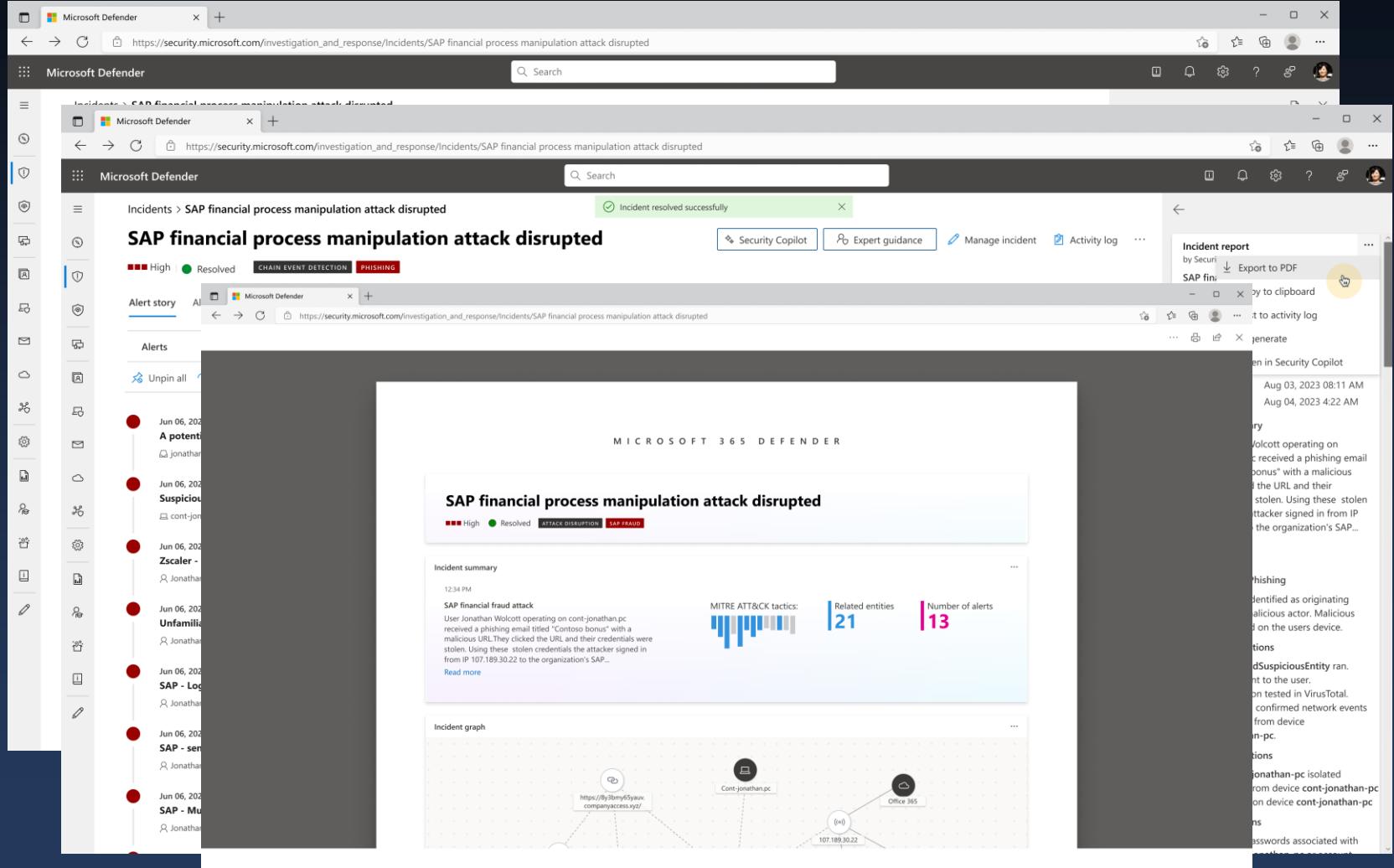
Guided incident investigation & response

- Understand the attack story in seconds with **incident summaries** and **asset summaries**
- Follow step-by-step expert guidance customized to your workflows to respond +easily contact the user



Guided incident investigation & response

- Understand the attack story in seconds with **incident summaries** and **asset summaries**
- Follow step-by-step expert guidance customized to your workflows to respond +easily contact the user
- Generate a summarized incident activity report and export to PDF



Natural Language Query Assistant

- Generate KQL queries to **hunt** in your environment using natural language

The screenshot shows the Microsoft Defender Data Explorer interface. On the left, a sidebar lists various data sources under 'Microsoft Defender (USX)'. In the center, a query editor displays the following KQL code:

```
let domains = dynamic(['bing.com', 'bing.com', 'bing.com']);
search in (EmailUrlInfo,UriClickEvents,DeviceNetworkEvents,DeviceFileEvents,DeviceEvents,BehaviorEntities)
Timestamp between (ago(180d) .. now())
and (RemoteUrl in ('domains'))
or FileOriginUrl in ('domains')
or FileOriginReferrerUrl in ('domains')
or Url in ('domains'))
and ActionType == "ConnectionSuccess"
| project $table, Timestamp, ActionType, DeviceId, DeviceName, RemoteUrl, InitiatingProcessFileName, RemoteIP, RemotePort,
InitiatingProcessSHA1, InitiatingProcessAccountName
```

Below the query, the 'Results' tab is selected, showing two rows of data:

Timestamp (UTC)	Table	Action type	DeviceId	Device name	Remote URL	Remote port
Jun 06, 2023 3:36 AM	DeviceNetworkEvent	ConnectionSuccess	6873-0r7689987...	cont-sarah.pc	intranet-host.cc	433
Jun 06, 2023 3:36 AM	DeviceNetworkEvent	ConnectionSuccess	6873-0r7689987...	cont-sarah.pc	intranet-host.cc	433

On the right, the 'Security Copilot' panel provides AI-generated context and recommendations:

- Aug 01, 2023 2:41 AM: Find any activities involving domains: ap.node-protection.cc, intranet-host.cc, vm.encrypted-network.cc
- Aug 01, 2023 2:41 AM: 8 attempts of connecting to device cont-sarah.pc in your tenant observed, 2 connections were successful
- Aug 01, 2023 2:41 AM: Show only successful connections
- Aug 01, 2023 2:41 AM: 2 successful connection attempts found from potential actor domains to cont-sarah.pc

At the bottom right, there is a text input field: "Ask anything about data exploration" with a blue arrow icon.

Script Analyzer

- Reverse engineer potentially malicious scripts in seconds with the Copilot script analyzer
- and now – analyze and malicious file too!

File analysis
Nov 15, 2023 08:36 AM

Overview

The file analysis report reveals that the file is potentially a Potentially Unwanted Application (PUA) bundler, specifically identified as PUABundler:Win32/ICBundler. This determination is based on the scan results from 5 out of 23 scanners, with a confidence level of 0.999. The file is signed by Lavsoft Software Canada Inc., with a valid digital certificate. The Portable Executable (PE) information shows an entry point address of 84180 and an image size of 192512. Strings analysis indicates that the file is related to the WebCompanionInstaller, with several strings referencing installation and uninstallation procedures. API analysis reveals risky API calls, such as CreateProcessAsUser and ShellExecuteExA, which can be used to execute processes with elevated privileges. The file also contains numerous references to registry manipulation, file operations, and internet communication, which could pose security risks.

Possible exfiltration to a malicious domain

Alert state

Classification	Assigned to
Not set	Unassigned
Set classification	Assign to

Alert details

Category	Techniques
Exfiltration	Exfiltration
Service source	Detection source
Microsoft 365 Defender	MDE
Generated on	First activity
06:46:03.722 AM	04:45:13.003 AM
Last activity	
06:46:03.722 AM	

Description

The file contains several strings related to the WebCompanionInstaller, such as "WebCompanionInstaller.exe", "InstallationStep", "WebCompanionInstaller.AppCore", and "InstallationException". These strings suggest that the file is involved in the installation and uninstallation of a software called WebCompanion. Additionally, strings like "CreateNotificationBlacklistStep", "GetFeatureFlagDataStep", and "ReplaceRegistryLocationStep" indicate that the file may perform various operations, such as modifying registry entries and managing feature flags.

API calls

The file makes use of risky API calls, such as CreateProcessAsUser and ShellExecuteExA, which can be used to execute processes with elevated privileges. These APIs can potentially be exploited for malicious purposes, such as running malware or gaining unauthorized access to system resources. Additionally, the file contains numerous references to registry manipulation (e.g., RegOpenKeyEx, RegCloseKey, RegQueryValueEx), file operations (e.g., DeleteFileW, CreateDirectoryW, FindFirstFileW), and internet communication (e.g., HttpWebRequest,WebResponse), which could pose security risks if misused.

Certificate

The screenshot shows the Microsoft Defender interface for investigating a SAP financial process manipulation attack. The main pane displays a network graph with nodes representing users (Jonathan Wolcott, cont-sarah.pc), hosts (SAP-01-Host, SAP-01), and external domains (Office 365, CosmicLynx, ap.node-production.cc). A specific alert is highlighted: "Possible exfiltration to a malicious domain" (High priority, In progress). The alert details pane shows a timeline of events, including a PowerShell script execution at 04:45:01.006 AM and 04:45:13.003 AM. The command line for the second event is: powershell.exe -NonInteractive -windowstyle hidden -enc JHBlhdgpgPSALXFxTQVAtmDFcaW50ZXJuYnxZ09jcyIgIA0K3URPQy5wZG1YDQoKZG9jM1A9IC3TQVAtRE90XzalnbkZ1INC3M6XH1XBcZG1hZ25v3RpYMuemlw1A1D0okd2v1C2vymz018VYAuabmK251wc90Zwh0a0wUlmJ12Ryb31DQpd0385I1Rza6FyZBhdhcJGRvvYE11CE2XMa0h5hd1vb1A1Qpc0S1JdGVIC1QXR0IC1k2hhcmVQYRoxCRkb2XkIIAtRGVzdC. The file path is C:\Program Files (x86)\Microsoft\Edge\Application\userin.exe and the SHA1 hash is 7c36a2c5a7d5c7e5c5f5f727eb583f91ce3968d.

New product highlights for General Availability

Customize and manage Copilot for Security for your security and IT team's daily operations



Custom promptbooks

Create custom promptbooks based on your data sources and procedures, each promptbook running the series of prompts your team follows to accomplish workstreams.



Knowledgebase integration

Your business logic can be integrated to empower Copilot for Security to perform activities based on your step-by-step guides.



Admin usage reporting

Review your team's product usage to forecast spending and inform provisioning.



Language availability

Model available in 8 languages and user experience available in 25.*

Under NDA only

*English, German, Japanese, Spanish, French, Italian, Portuguese, and Chinese in model and in addition, Korean, Dutch, Swedish, Polish, Norwegian, Turkish, Danish, Finnish and more in UX.

Customer experiences..



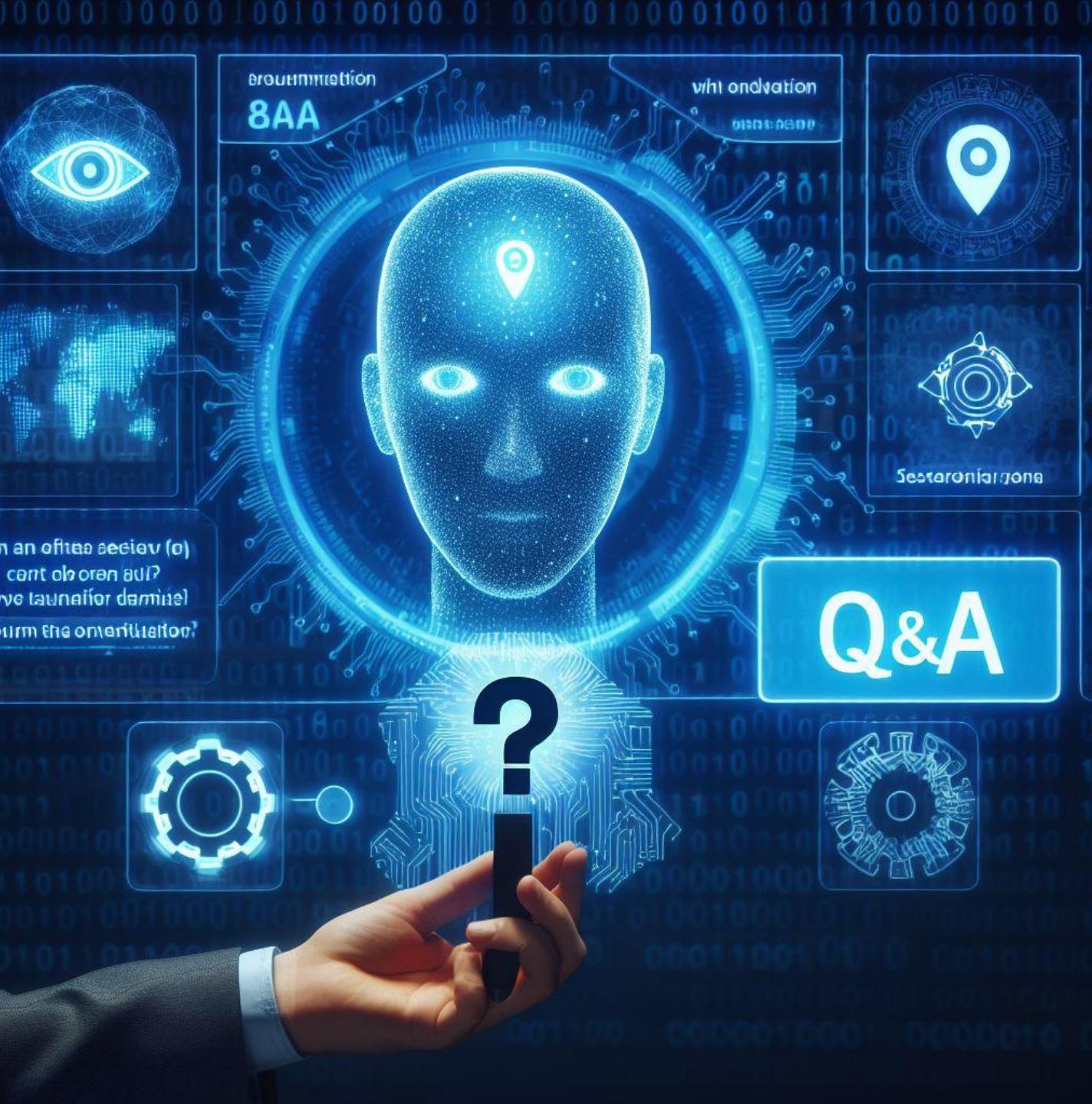
Pricing

Security Compute Unit (SCU)

(1 SCU = \$4 / hour = \$2.920 / month)



Q&A



Closing

- **What's beyond the tip of the iceberg**
- **Meet us at the Booth**
- **Try it out**

