

Copilot for Security: Identity security cookbook

Darko Todoroski Cybersecurity Solution Architect

Mirad Maglic Cybersecurity Sales Executive

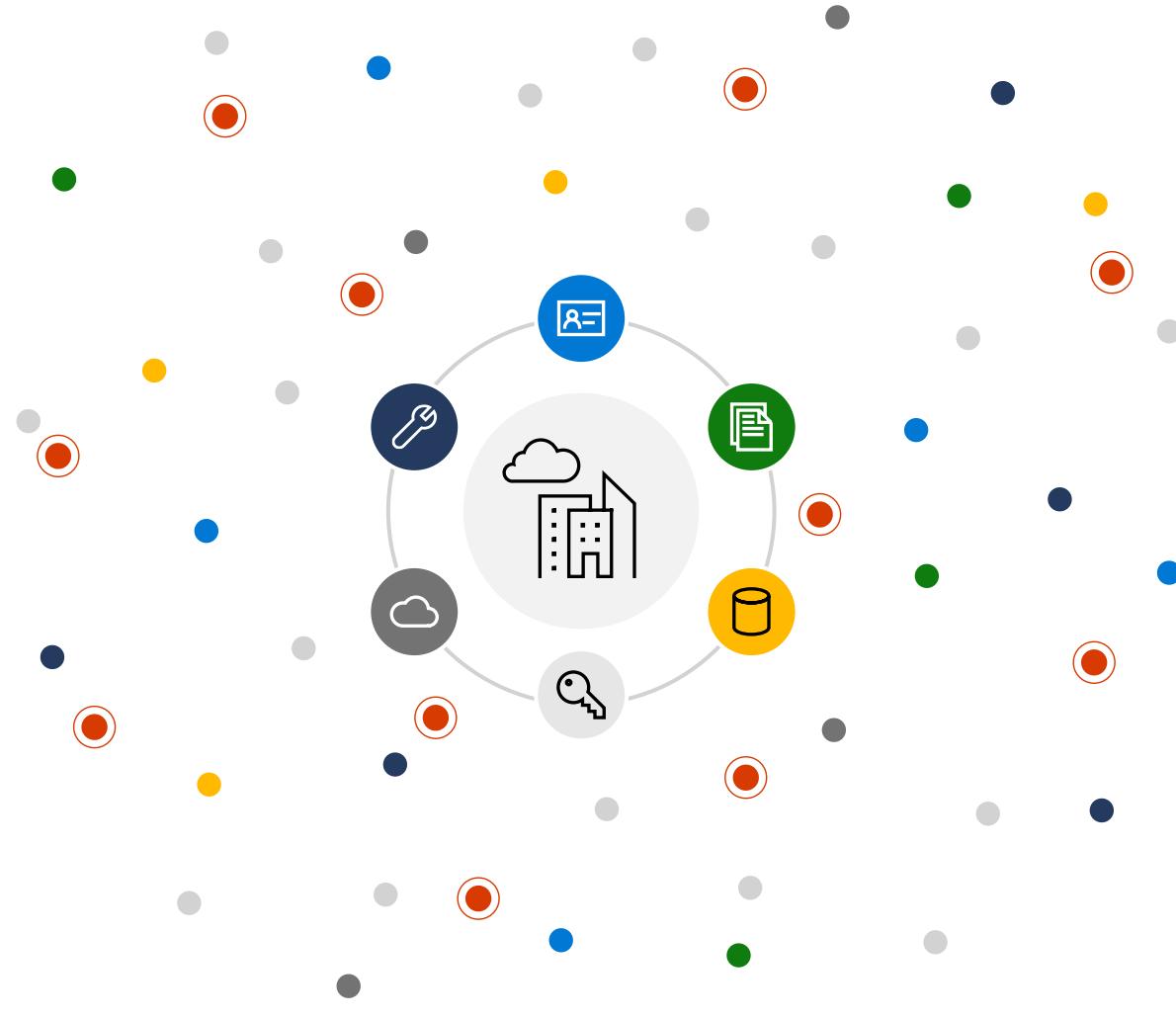


Agenda

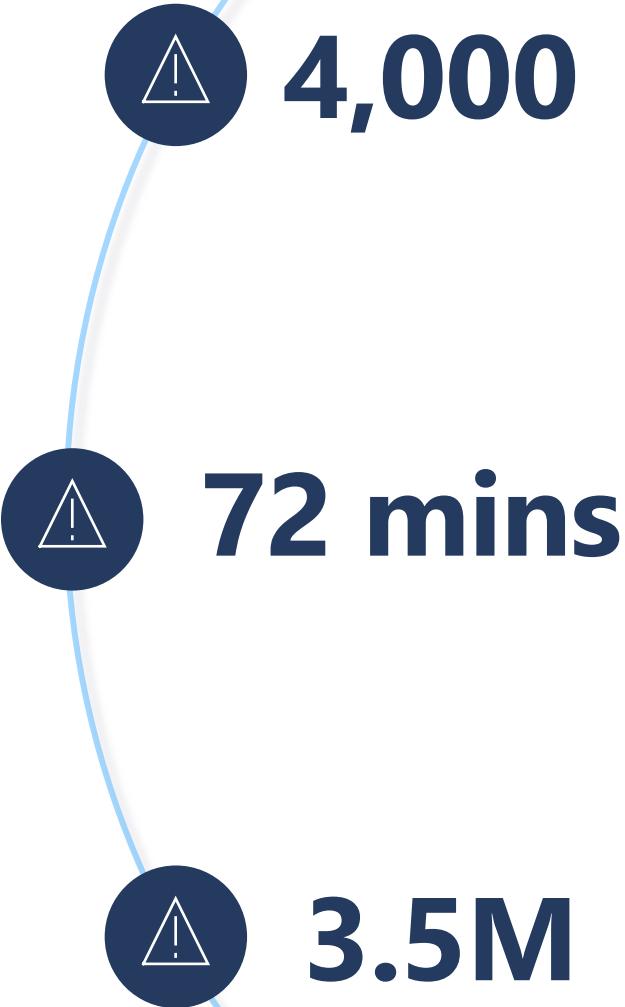
- Who are we?
- Identity security challenges of today
- Why GenAI for identity protection?
- Use cases / demos
- The anatomy of a great prompt

Today's digital landscape and its challenges

- » Rapid increase of identities that need to be protected
- » Accelerated growth of apps, on and off the corporate network, requiring secure access
- » Hybrid work requires seamless, flexible experience while keeping access secure
- » Evolving regulations with data privacy and security implications



The odds are
against today's
security analysts

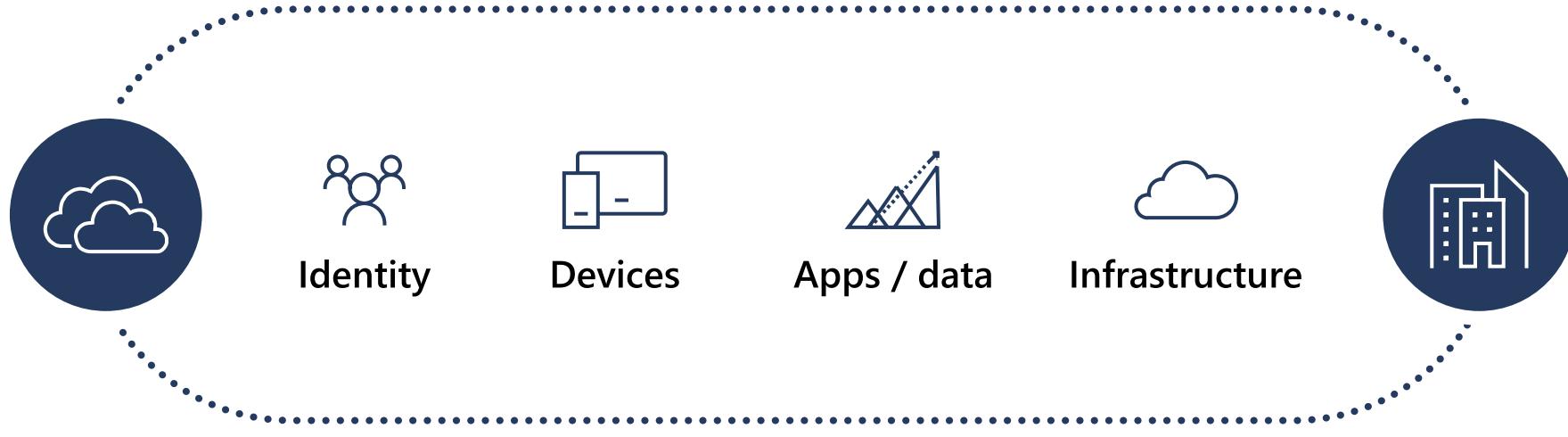


Password attacks per second

Median time for an attacker to access your private data if you fall victim to a phishing email

Global shortage of skilled cybersecurity professionals

Identity security imperatives



Visibility

Understand the security state
and risks across resources

Control

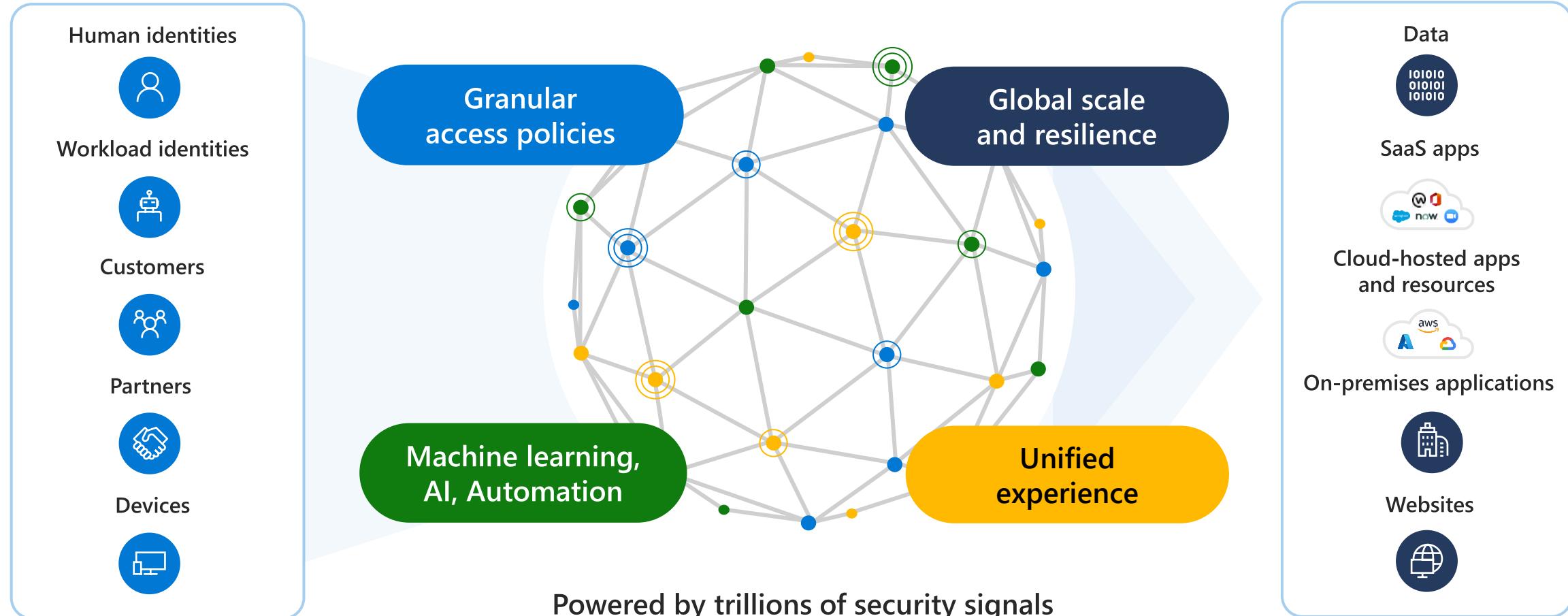
Define consistent security
policies and enable controls

Guidance

Elevate security through built-in
intelligence and recommendations

Strengthen defenses against attackers with Microsoft Entra

Every identity | Every resource | Everywhere



Microsoft Entra product family

Secure access for a connected world

**Identity
and access
management**

Microsoft Entra ID
(formerly Azure AD)



Microsoft Entra
ID Governance



Microsoft Entra
External ID



Microsoft Entra
Internet Access



Microsoft Entra
Private Access



Network access

**New
identity
categories**

Microsoft Entra
Verified ID



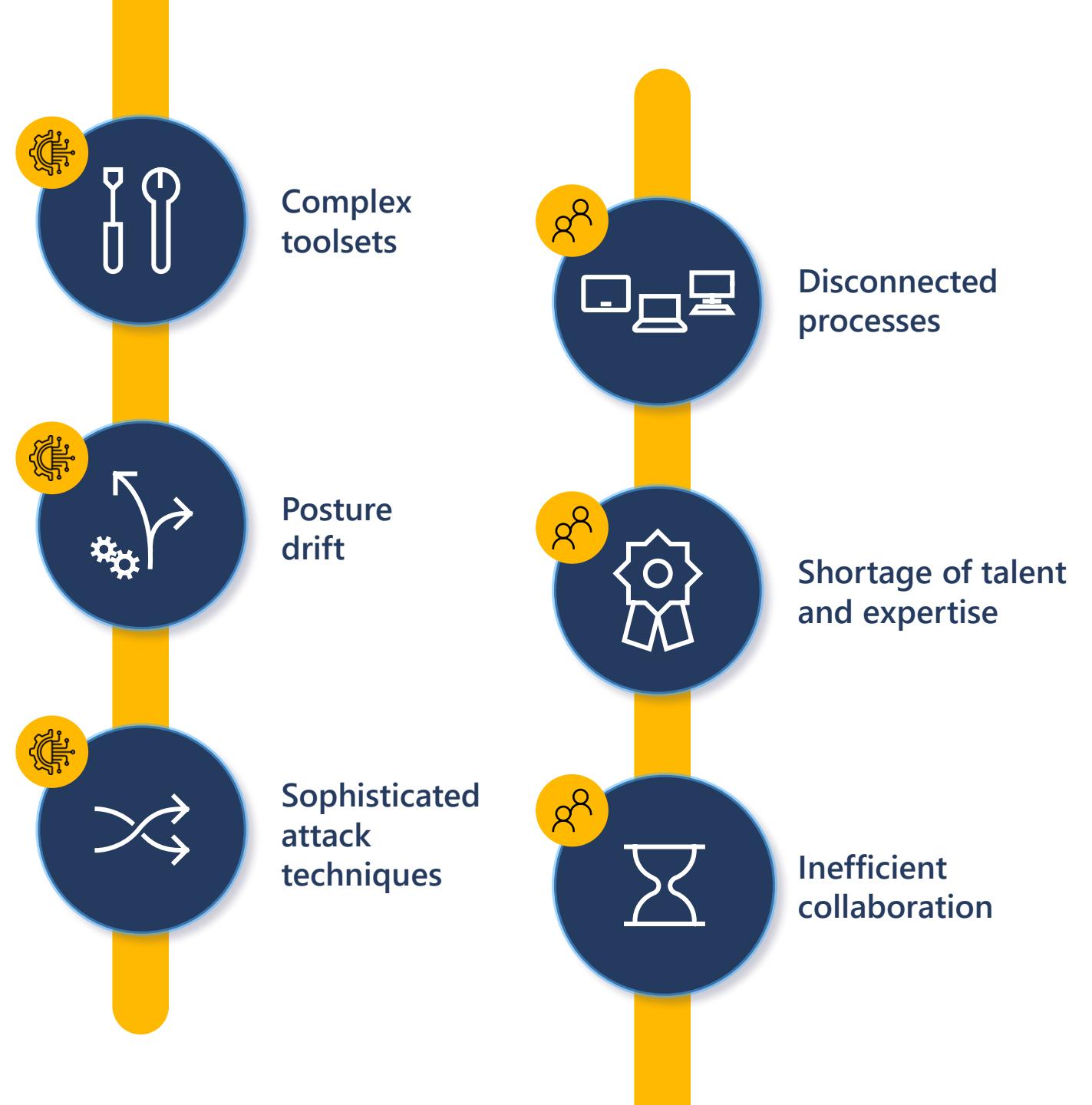
Microsoft Entra
Permissions
Management



Microsoft Entra
Workload ID



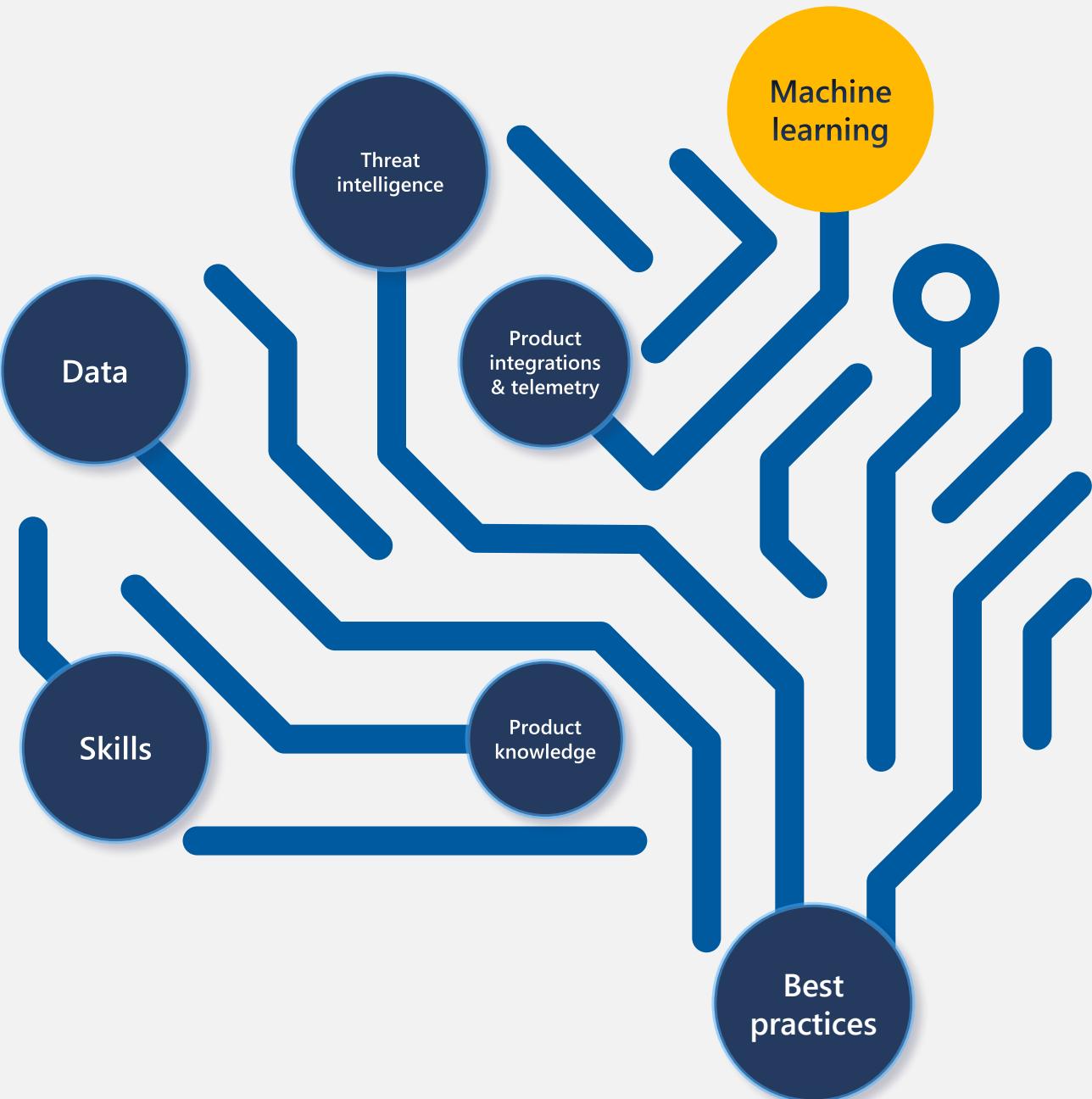
Defenders need a new approach



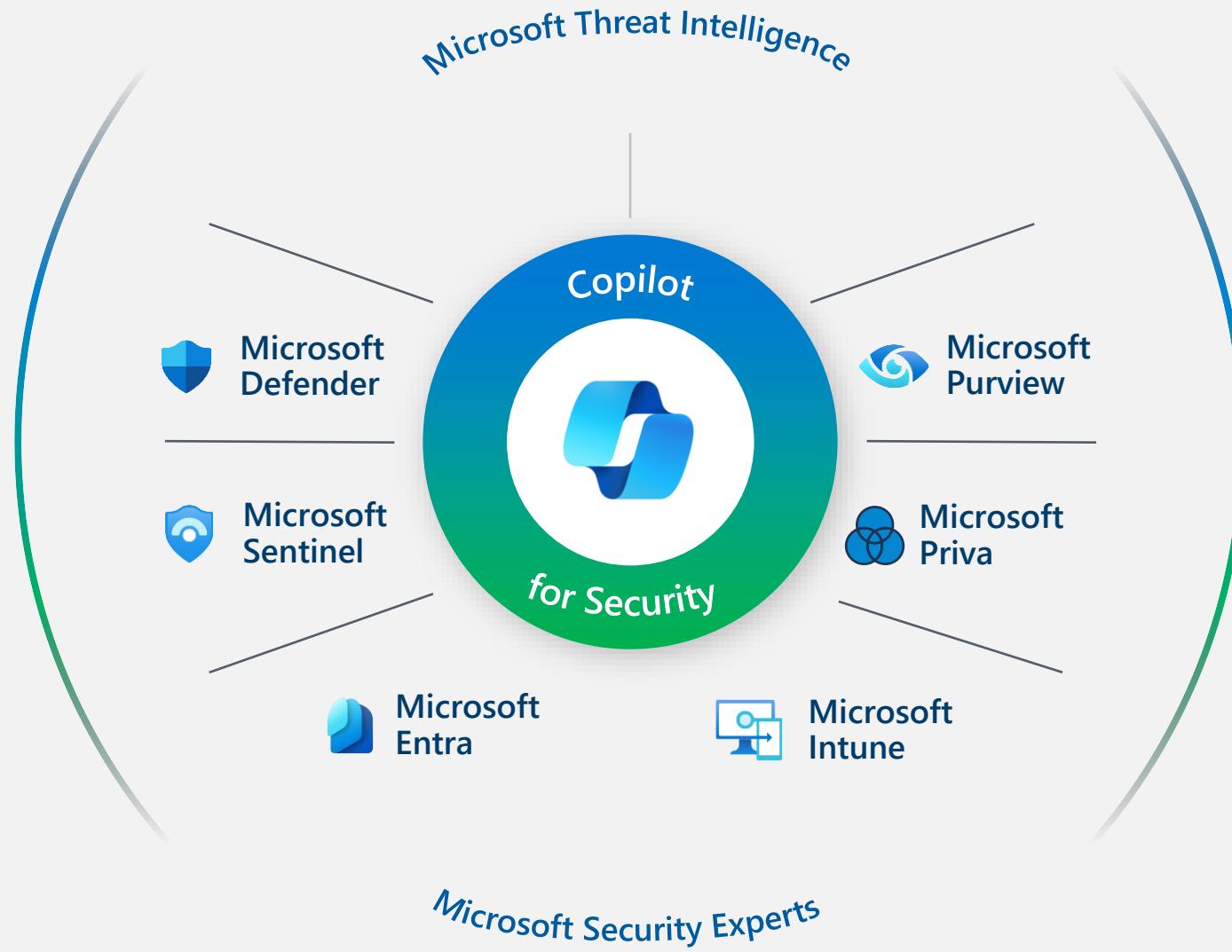


Microsoft Copilot for Security

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



Microsoft's End-to-End Security



Microsoft Copilot for Security improves speed, accuracy and sentiment

Security professionals with Copilot were...



22%

faster

Security professionals with Copilot were...



7%

more accurate

Security professionals want to use Copilot...



97%

reported they want Copilot next time they do the same task

Show of hands

Raise your hand if you are responsible for securing identities in your organisation...

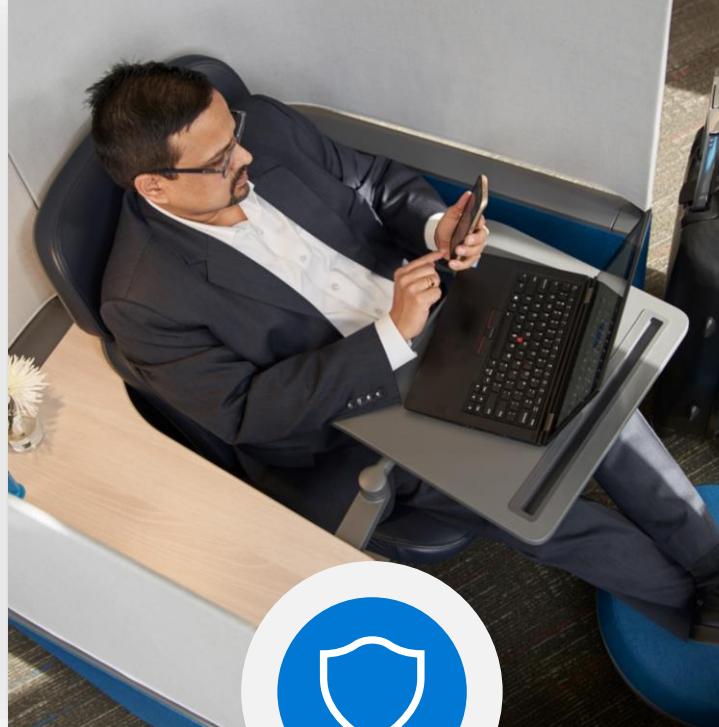
...and you are confident you can uncover and fix all identity related threats and incidents? ☺



Simplified identity governance



Automate the Identity Lifecycle



Strengthen Security,
Improve Productivity



Support on-premises and
cloud apps

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 sidebar with "Insider Risk Management" and various navigation options. In the center, there's a card for an alert titled "(7bbc3040) Data theft by departing users".

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

Triggering event:
Sept 25, 2023 (RTG)
An HR connector imported a resignation date for this user.

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

User alert history:
Last 10 days
Data theft for departing employees (1 alert)
Sensitive info leak (1 alert)
Security violations (1 alert)
View all alert history

Summary | **Activity explorer** | **User activity** | **Forensic evidence**

At the bottom, there's a "Security Copilot" card with a "Natural language prompt" field containing the query "Find Mona Kane and Anne Keetings' documents and emails that contain the word 'Reader' within 2 words of '1.0' or the phrase 'MS Reader', or the word 'Reader' within 10 words of 'Microsoft'." There are also "Featured prompts", "Refine", "Revert", "AI generated. Verify for accuracy.", and "Generate KQL" buttons.

Security Copilot embedded experiences

The screenshot shows the Microsoft Azure interface with the Microsoft Defender for Cloud Recommendations blade open. A modal window titled "Security Copilot" is displayed, providing detailed information about publicly exposed resources.

Microsoft Defender for Cloud | Recommendations

Active recommendations by risk

Risk level	Critical	High	Medium	Low	N/A
Count	48	55	180	1297	3448

Other metrics

Category	Value
Active attack paths	216
Affected resources	1811
Overdue recommendations	342

Defender resource coverage

Status	Count
Full 105	105
Partial 105	105
Not covered 207	207

Security Copilot

Show critical risks to publicly exposed resources

Aug 01, 2023 11:14 AM

13 publicly exposed resources require attention

There are 13 publicly exposed resources, each carrying a range of potential threats such as unmanaged workloads, human errors, misconfigurations, data breaches, privacy and compliance issues, performance degradation, and security vulnerabilities.

Here's a breakdown of the specific resources at risk:

- 9 VMs with internet exposure and high severity vulnerabilities
- 1 AWS S3 bucket that's publicly accessible, housing sensitive data
- 1 SQL with excessive internet exposure, allowing basic authentication and containing sensitive data
- 2 API endpoints lacking authentication, transmitting sensitive information.

See less

Show results

AI generated. Verify for accuracy.

Focus on risks to sensitive data

Focus on risks to critical vulnerability

Focus on risks to lateral movement

<Helper text here>

[Home](#)[Favorites](#)[Identity](#)[Protection](#)[Identity governance](#)[Dashboard](#)[Entitlement management](#)[Access reviews](#)[Privileged Identity Management](#)[Lifecycle workflows](#)[Verifiable credentials](#)[Permissions Management](#)[Global Secure Access \(Preview\)](#)[Learn & support](#)

Home >

Lifecycle workflows | Overview

Identity Governance



Search

Create workflow

Got feedback?

Getting Started

Overview

Copilot can help

Workflows

[Workflows](#)[Deleted workflows](#)

Manage

[Custom extensions](#)[Workflow settings](#)

No alerts to display

Activity

[Audit logs](#)

Workflow schedule

Every 1 hours

[View workflow settings](#)

Schedule enabled

9

[View workflows](#)

Schedule disabled

8

[View workflows](#)

Deleted workflows

4

[View deleted workflows](#)

Quick Actions

[View workflows](#) [Create workflow](#)



Overview

Workflows

Workflows

Deleted workflows

Manage

Custom extensions

Workflow settings

Activity

Audit logs

Troubleshooting + Support

Troubleshoot

New support request

Getting Started

Overview



Copilot can help

Alerts

No alerts to display

My Feed



Workflow schedule

Every 1 hours

[View workflow settings](#)

Schedule edits

9

[View workflow](#)

Schedule disabled

8



Deleted workflows

4

Copilot Assisted Lifecycle Workflow Insights

Quickly get rich insights to help monitor and troubleshoot workflows

Summary

Start monitoring workflow execution with a succinct summary of the most relevant workflow run information.

Context

Use suggested prompts to discover even more processing insights in the current context.

Details

See a detailed view of user specifics over a desired time period to investigate further or troubleshoot if needed.

Tell me how many times my workflow was run recently

Follow up prompts to get more contextual insights

Summarize what happened for a specific user in this workflow

Additional prompts to explore further

How many times did the 'Government Sales employee onboarding' workflow run in the last 24 hours?

The 'Government Sales employee onboarding' workflow ran a total of 8 times in the last 24 hours. Out of these runs, 5 were successful and 3 failed. The workflow attempted to process a total of 38 tasks, out of which 7 tasks failed. The workflow was run for a total of 9 users.

AI-generated content may be incorrect



7 of 15 requests

Which users were processed in these runs?

In the last 24 hours, the 'Government Sales employee onboarding' workflow processed the following users:

1. User with ID 'ce817d62-54b8-4c1f-a0d2-114b95a33342' was processed multiple times. The processing statuses were 'completed', 'completedWithErrors', and 'failed'.
2. User with ID 'fa9bcd58-d0d5-4164-a365-3b6f307dc077' was also processed multiple times. The processing statuses were 'completed', 'completedWithErrors', 'failed', and 'completedWithErrors'.

Please note that the 'completedWithErrors' status indicates that the workflow run completed, but one or more tasks within the run encountered errors. The 'failed' status indicates that the workflow run did not complete successfully.

AI-generated content may be incorrect



8 of 15 requests

Summarize the runs for user fa9bcd58-d0d5-4164-a365-3b6f307dc077 for the 'Government Sales employee onboarding' workflow in the last 7 days?

In the last 7 days, the 'Government Sales employee onboarding' workflow processed the user with ID 'fa9bcd58-d0d5-4164-a365-3b6f307dc077' multiple times. Here are the details:

1. Workflow run completed with no failed tasks. (Version: 4, Execution Type: onDemand, Completed DateTime: 2024-03-01T18:34:41.201915Z)
2. Workflow run failed with 1 failed task. (Version: 4, Execution Type: onDemand, Completed DateTime: 2024-03-01T18:30:03.4440229Z)
3. Workflow run completed with errors, 1 task failed.

What tasks are included in the 'Government Sales employee onboarding' workflow?

How can I modify the 'Government Sales employee onboarding' workflow?

What does the 'Request user access package assignment' task do?

Copilot Assisted Lifecycle Workflow Insights

Quickly get rich insights to help monitor and troubleshoot workflows

Summary

Start monitoring workflow execution with a succinct summary of the most relevant workflow run information.

Context

Use suggested prompts to discover even more processing insights in the current context.

Details

See a detailed view of user specifics over a desired time period to investigate further or troubleshoot if needed.

Compare workflows versions for a specific workflow

Summarize what changed on this workflow

Additional prompts to explore further

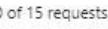
What's the difference between version 2 and version 4 of the 'Government Sales employee onboarding' workflow?

The 'Government Sales employee onboarding' workflow has undergone some changes between version 2 and version 4. Here are the key differences:

- Version 2:
 - Last Modified: 2024-03-01T18:20:43.1095559Z
 - Created: 2024-03-01T18:15:17.2031814Z
 - Execution Conditions: Triggered based on the 'employeeHireDate' attribute with no offset in days. The scope is set for users in the 'Government Sales' department in the 'US'.
 - Tasks: The workflow consists of 5 tasks including 'Enable User Account', 'Send Welcome Email', 'Add user to groups', 'Request user access package assignment', and 'Generate TAP and Send Email'.
- Version 4:
 - Last Modified: 2024-03-01T18:28:09.7550809Z
 - Created: 2024-03-01T18:28:09.7550826Z
 - Execution Conditions: The conditions remain the same as in version 2.
 - Tasks: The workflow consists of 4 tasks including 'Enable User Account', 'Send Welcome Email', 'Add user to groups', and 'Request user access package assignment'. The 'Generate TAP and Send Email' task present in version 2 is not included in this version.

Please note that the 'Enable User Account' task is common to both versions and is used to enable the user account in the directory. The 'Send Welcome Email' task sends a welcome email to the new hire. The 'Add user to groups' task adds the user to selected groups. The 'Request user access package assignment' task requests user assignment to a selected access package. The 'Generate TAP and Send Email' task, present only in version 2, generates a Temporary Access Pass and sends it via email to the user's manager.

AI-generated content may be incorrect



• 10 of 15 requests

What tasks are included in the 'Government Sales employee onboarding' workflow?

How can I modify the 'Government Sales employee onboarding' workflow?

What does the 'Request user access package assignment' task do?

I want to ...

0 / 500







InPrivate



Sign in to your account

x

+

-

□

x

<https://login.microsoftonline.com/common/reprocess?ctx=rQQIARAfZH...>

balas@contoso.com

You can't get there from here

This application contains sensitive information and can only be accessed from:

- Devices or client applications that meet Contoso management compliance policy.

You need to be signed in to Microsoft Edge with the work or school account shown above. To sign in, click on your account image. [Learn More](#)

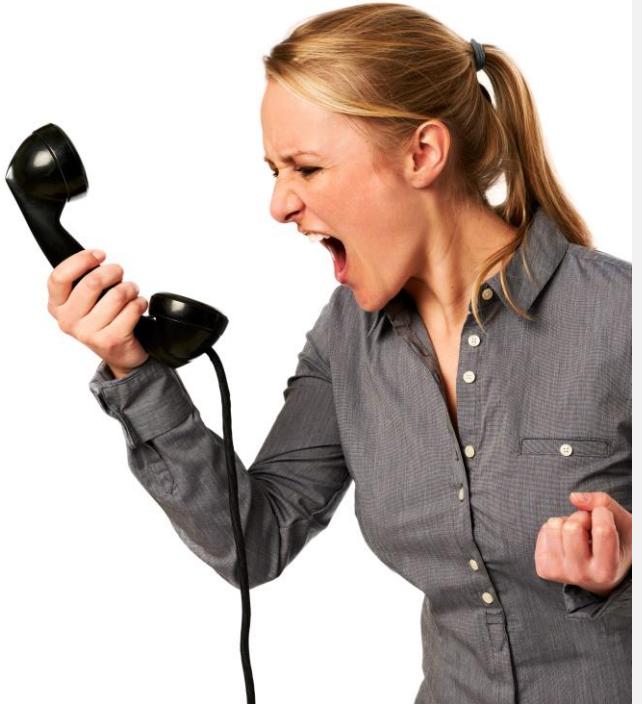
If you're not planning to do this right now, you might still be able to browse to other Contoso sites. Otherwise, [sign out](#) to protect your account.

[Sign out and sign in with a different account](#)

[More details](#)

[Terms of use](#)[Privacy & cookies](#)

...



InPrivate

Sign in to your account

https://login.microsoftonline.com/common/reprocess?ctx=rQQIARAfZH...

You need to be signed in to Microsoft Edge with the work or school account shown above. To sign in, click on your account image. [Learn More](#)

If you're not planning to do this right now, you might still be able to browse to other Contoso sites. Otherwise, [sign out to protect your account](#).

[Sign out and sign in with a different account](#)

[More details](#)

Request Id: 41609ed3-8b57-413e-9f9d-318ede0000

Correlation Id: 52d58191-67d8-494a-87af-c1ec31e663a1

Timestamp: 2020-03-26T00:53:52.854Z

App name: Azure Portal

App id: c44b4083-3bb0-49c1-b47d-974e53cbdf3c

IP address: 73.83.66.107

Device identifier: Not available

Device platform: Windows 10

Device state: Unregistered

Advanced diagnostics: [Enable](#)

If you plan on getting support for an issue, turn this on and try to reproduce the error. This will collect additional information that will help troubleshoot the issue.

Terms of use Privacy & cookies ...

Home

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity governance

External Identities

Show more

Protection

Identity governance

Verifiable credentials

Permissions Management

Global Secure Access (Preview)

Learn & support

Home >

Sign-in events

Download Export Data Settings Troubleshoot Refresh | Columns | Got feedback?

This view will be soon replaced with a view that includes refresh tokens and application sign-ins. Try out our new sign-ins preview. →

Date : Last 1 month

Show dates as : Local

Add filters

Date	Request ID	User	Application	Status	IP address	Location	Conditional Acc...	Authentication r...
10/27/2023, 6:58:02 ...	54444578-337d-40a...	S***** V***	Microsoft App Acces...	Interrupted	1**.2**.1**.4**	Narayan Peth, Mahar...	Failure	Multifactor authentic...
10/27/2023, 6:57:58 ...	3ea7011b-01a6-419...	On-Premises Directo...	Microsoft Azure Acti...	Success	20.25.176.197	Phoenix, Arizona, US	Not Applied	Single-factor authen...
10/27/2023, 6:57:49 ...	b51ca60f-31e5-4c3b...	On-Premises Directo...	Microsoft Azure Acti...	Success	20.25.176.197	Phoenix, Arizona, US	Not Applied	Single-factor authen...
10/27/2023, 6:53:02 ...	7328be9f-9672-447f...	S***** V***	Microsoft App Acces...	Interrupted	1**.2**.1**.4**	Narayan Peth, Mahar...	Failure	Multifactor authentic...
10/27/2023, 6:52:52 ...	fa1d88bf-3dc1-4748...	J**** C***** (****...	Office365 Shell WCS...	Success	2**.2**.3**.1**	Bellevue, Washingto...	Success	Multifactor authentic...
10/27/2023, 6:52:52 ...	289813c1-429f-40a5...	J**** C***** (****...	Office365 Shell WCS...	Success	2**.2**.3**.1**	Bellevue, Washingto...	Success	Multifactor authentic...
10/27/2023, 6:52:52 ...	ba5d6658-bfea-44b...	J**** C***** (****...	Office365 Shell WCS...	Success	2**.2**.3**.1**	Bellevue, Washingto...	Success	Multifactor authentic...
10/27/2023, 6:52:46 ...	f4b84dbb-cd3e-49f5...	J**** C***** (****...	Microsoft 365 Securi...	Success	2**.2**.3**.1**	Bellevue, Washingto...	Success	Multifactor authentic...
10/27/2023, 6:52:04 ...	98fdf4ed-296a-4ee7...	J**** C***** (****...	Azure Portal	Success	2**.2**.3**.1**	Bellevue, Washingto...	Success	Multifactor authentic...
10/27/2023, 6:48:02 ...	fd60b0f5-8692-4e74...	S***** V***	Microsoft App Acces...	Interrupted	1**.2**.1**.4**	Narayan Peth, Mahar...	Failure	Multifactor authentic...
10/27/2023, 6:47:34 ...	291b4759-f665-4e9c...	S**** L****	CAttack	Success	2**.2**.3**.1**	Sydney, New South ...	Success	Single-factor authen...
10/27/2023, 6:47:32 ...	d7a5f60b-f6be-468e...	P**** F*****	CAttack	Success	2**.2**.3**.1**	Sydney, New South ...	Success	Single-factor authen...
10/27/2023, 6:44:30 ...	d80de78c-1b7b-4a7...	On-Premises Directo...	Microsoft Azure Acti...	Success	20.36.24.253	Quincy, Washington,...	Not Applied	Single-factor authen...
10/27/2023, 6:44:11 ...	cafe179-d451-4ea5...	On-Premises Directo...	Microsoft Azure Acti...	Success	20.36.24.253	Quincy, Washington,...	Not Applied	Single-factor authen...
10/27/2023, 6:43:38 ...	f0f1f6a1-30d5-4749...	S**** L****	CAttack	Success	2**.2**.3**.2**	Sydney, New South ...	Success	Single-factor authen...
10/27/2023, 6:43:35 ...	7b9ff23d-8290-4426...	D**** H*****	CAttack	Success	2**.2**.3**.2**	Sydney, New South ...	Success	Single-factor authen...
10/27/2023, 6:43:22 ...	60eae47e-1b0e-44b...	J**** R**	Portal View	Success	4**.6**.1**.9**	Quincy, Washington,...	Not Applied	Single-factor authen...
10/27/2023, 6:43:03 ...	b3ff82fb-1868-4c3c...	S***** V***	Microsoft App Acces...	Interrupted	1**.2**.1**.4**	Narayan Peth, Mahar...	Failure	Multifactor authentic...
10/27/2023, 6:42:36 ...	7ed691f2-cc29-4c69...	J**** R**	Portal View On	Success	4**.6**.1**.9**	Quincy, Washington,...	Not Applied	Single-factor authen...
10/27/2023, 6:38:41 ...	01cf31a9-d39d-4025...	W***** W***	Azure Portal	Success	4**.1**.1**.5**	Quincy, Washington,...	Success	Multifactor authentic...
10/27/2023, 6:28:02 ...	91-51726-750-4f1...	S***** V***	Microsoft App Acces...	Interrupted	1**.2**.1**.1**	Narayan Peth, Mahar...	Failure	Multifactor authentic...



Copilot

Preview

...

X

sign-in attempt is not compliant and is not managed.

The authentication method used was Password Hash Sync, but it did not succeed due to the user account being disabled.

Please note that this information is based on the most recent data available and may not include all sign-in attempts.



1 of 10

Why was Lynne Robbins prompted for MFA? RequestID: a3179d22-b746-4273- b0b7-cb8a81c9f400?

Lynne Robbins was prompted for Multi-Factor Authentication (MFA) during a sign-in attempt on October 17, 2023, at 10:40:06 UTC. The sign-in attempt was made from an IP address located in Washington, Virginia, USA. The IP address is 138.91.108.57. The sign-in attempt was made using the "My Apps" application.

The MFA prompt was triggered due to the enforcement of a Conditional Access policy named "CA33 - AlpineUser MFA or Device". This policy requires either MFA or a device to be enforced. In this case, MFA was enforced.

However, the sign-in attempt failed due to the user account being disabled. The user object in Active Directory backing this account has been disabled. An admin can re-enable this account through Powershell.

The sign-in attempt was made using a Windows 10 operating system and the Edge 118.0.2088 browser. The device used for the sign-in attempt is not compliant and is not managed.

Please note that this information is based on the most recent data available and may not include all sign-in attempts.



2 of 10

What is the MFA requirement policy? Are other users impacted? C

Enter your message here...



...

0/256



AI generated content may be incorrect.

InPrivate

Sign in to your account

https://login.microsoftonline.com/common/reprocess?ctx=rQQIARAAfZH...

 Microsoft

balas@contoso.com

Your account is blocked

We've detected suspicious activity on your account.

Sorry, the organization you are trying to access restricts at-risk users. Please contact your Contoso admin. [Learn more](#)

[Sign out and sign in with a different account](#)

[More details](#)

Terms of use Privacy & cookies ...

 Home Favorites Identity Protection Identity Protection Conditional Access Authentication methods Password reset Custom security attributes Risky activities Show more Identity governance Verifiable credentials Permissions Management Global Secure Access (Preview) Learn & support

Home > Identity Protection



Identity Protection | Risky users



Search



Learn more



Download



Select all



Confirm user(s) compromised



Dismiss user(s) risk



Refresh



Columns



Got feedback?



We recommend migrating Identity Protection policies to Conditional Access for more conditions and controls. Learn more →

Auto refresh : Off

Show dates as : Local

Risk state : 2 selected

Status : Active

Risk level : High, Medium

Add filters

 User ↑↓

Risk state ↑↓

Risk last updated ↑↓

 Joseph Run

At risk

10/26/2023, 5:39:16 PM

...

 Christer Ljung

At risk

10/25/2023, 2:34:30 PM

...

 Backup Admin (parkcity)

At risk

10/25/2023, 2:59:38 AM

...

 Bianca Pisani

At risk

10/24/2023, 5:30:19 PM

...

 Adell Evens (Project TNT)

At risk

10/24/2023, 2:40:30 AM

...

 Morgan Valentine

At risk

10/20/2023, 3:51:52 PM

...

 Lynne Robbins

At risk

10/17/2023, 12:09:13 PM

...

 Jonathan Wolcott

At risk

10/17/2023, 11:41:12 AM

...

 Lee Gu

At risk

10/16/2023, 4:07:59 PM

...

 Ashley Ramirez

At risk

10/16/2023, 9:08:03 AM

...

 Michael G Scott

At risk

10/14/2023, 2:38:25 PM

...

 Mercy Maina

At risk

10/3/2023, 9:26:22 PM

...

 James Carpenter (Zarmada LLC)

At risk

9/26/2023, 11:52:57 PM

...

 Jeff Barker

At risk

9/21/2023, 10:13:03 PM

...

 Leyna Ingold

At risk

9/21/2023, 5:12:12 PM

...

Load more

Home

Favorites

Identity

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Custom security attributes

Risky activities

... Show more

Identity governance

Verifiable credentials

Permissions Management

Global Secure Access (Preview)

Learn & support

Home > Identity Protection

Identity Protection | Risky users

Search



Learn more



We recommend migration

Auto refresh : **Off** User ↑↓ Joseph Run Christer Ljung Backup Admin (parking) Bianca Pisani Adell Evens (Project Manager) Morgan Valentine Lynne Robbins Jonathan Wolcott Lee Gu Ashley Ramirez Michael G Scott Mercy Maina James Carpenter (Zarathustra) Jeff Barker Leyna Ingold

Risky User Details

Reset password

Confirm user compromised

Dismiss user risk

Unblock 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 Lynne Robbins has three recent risky activities, all with Medium risk level.
- The risk detection type is Anomalous token.
- Anomalous token indicates abnormal characteristics in the token such as an unusual token lifetime or a token that is played from an unfamiliar location.
- Risky sign-in 1 (RequestId: 42e8fa1f-8adc-496d-a5db-1da3e7b8e900, CorrelationId: 89b0c74a-12fe-4de9-b855-2da6859cac7f) with Medium risk level occurred on 2024-02-27T16:12:17 UTC for Resource OfficeHome. The sign-in IP was 185.82.127.128 and location was Stockholm, Stockholms Lan SE. The IP, ASN, Location, Browser Id and Device Id were unfamiliar to the user. There was no MFA for this sign-in.
- Risky sign-in 2 (RequestId: 0a21a284-8de6-4609-a0ca-c81a330c5500, CorrelationId: 60bd1c7e-c276-4c15-9586-eefe2e01dba8) with Medium risk level occurred on 2024-02-17T22:19:39 UTC for Resource OfficeHome. The sign-in IP was 185.243.218.41 and location was Sandefjord, Vestfold NO. The IP, ASN, Location, Browser Id and Device Id were unfamiliar to the user. There was no MFA for this sign-in.
- Risky sign-in 3 (RequestId: 0ff84803-ff5c-4c20-8f28-ced19891c600) with Low risk level occurred on 2024-02-27T16:12:17 UTC for Application Browser and Resource OfficeHome. The sign-in IP was 185.82.127.128 and location was Stockholm, Stockholms Lan SE. The IP, ASN, Location, Browser Id and Device Id 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.

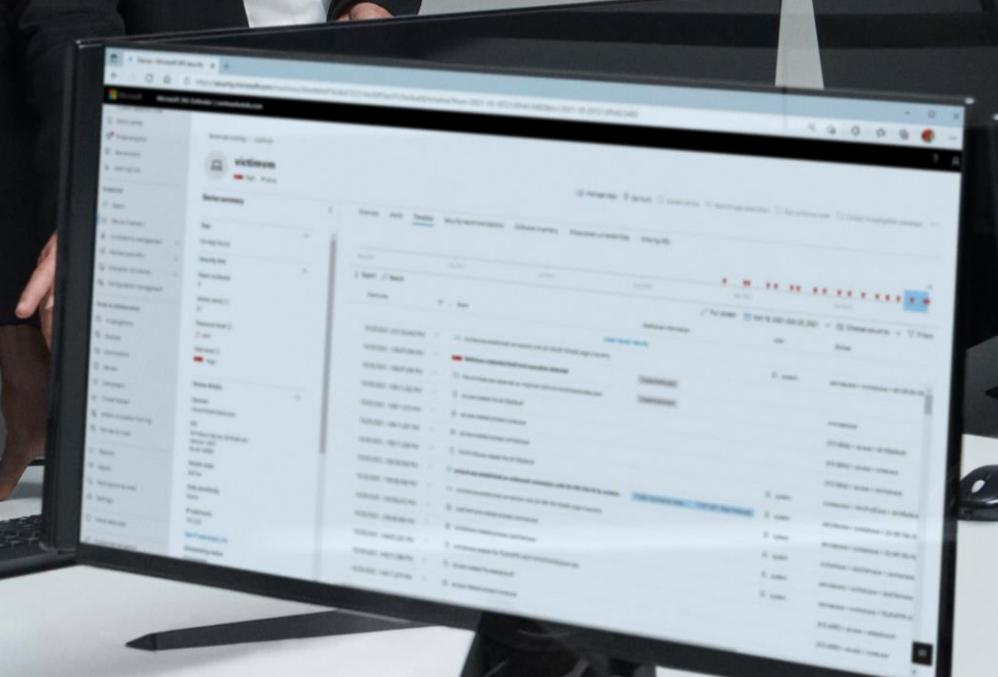
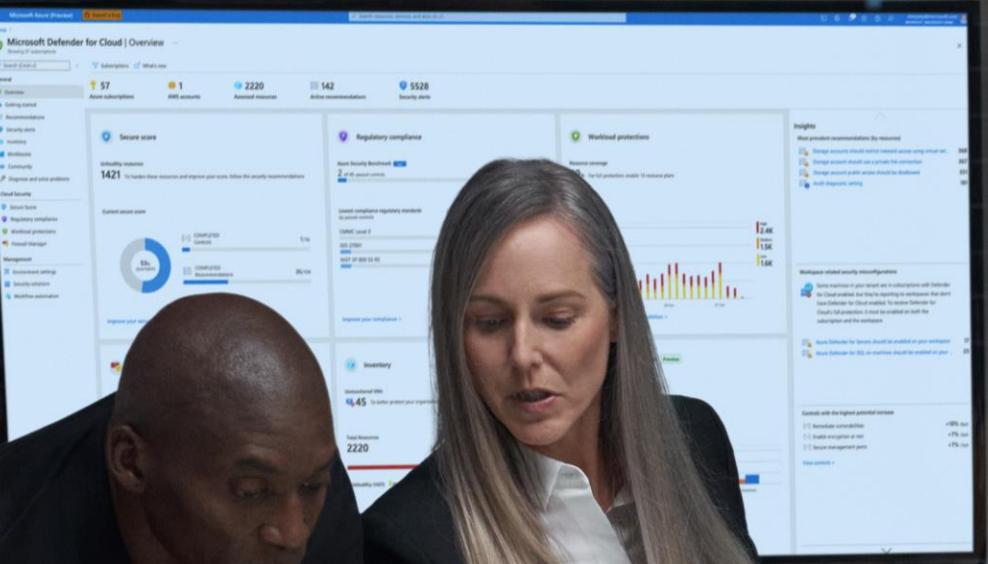
If you do not have those policies:

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?](#)



Get started with our interactive tour

Quickly learn essentials like prompting, pinning, and providing feedback—to get the most from your AI-powered assistant.

[Start tour](#)

Explore with Copilot

[❖ Featured prompts](#)[❖ Promptbooks](#)

Microsoft Sentinel incident investigation

Get a report about a specific incident, along with related alerts, reputation scores, users, and devices.

Microsoft Security · 7

Threat actor profile

Get a report profiling a known actor with suggestions for protecting against common tools and tactics.

Microsoft Security · 5

Vulnerability impact assessment

Get a report summarizing the intelligence for a known vulnerability and how to address it.

Microsoft Security · 6

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



Get started with our interactive tour

Quickly learn essentials like prompting, pinning, and providing feedback—to get the most from your AI-powered assistant.

[Start tour](#)

Explore with Copilot

[Featured prompts](#)[Promptbooks](#)

Show high severity Microsoft Defender XDR incidents.

[New Microsoft Defender XDR](#)

Summarize recent threat intelligence.

[New Microsoft Defender Threat Intelligence](#)

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





○ Status: The user account is disabled.

○ Applied Conditional Access Policies: CA33 - AlpineUser MFA or Device (success)

To re-enable the user account, an admin can use PowerShell as described in the [Enable-ADAccount](#) documentation.



Looks right



Needs improvement



Inappropriate



Is the user considered risky? If so why?



> 3 steps completed 26s

Oct 31, 2023 | 27.44s

Lynne Robbins (userId: 006a987e-6a0b-4891-a7b5-1277233e8bd4) is considered a risky user. She has a high risk level and her risk state is marked as "At Risk". However, there are no specific risk details provided to explain why she is considered risky. The risk information was last updated on October 17, 2023.



Looks right



Needs improvement



Inappropriate



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





actor and their intersection with ransomware

> 3 steps completed 47s

Oct 31, 2023 | 48.39s

Manatee Tempest (DEV-0243) is a Russia-based cybercriminal group that has been active since June 2014. It overlaps with the activity tracked by the cyber intelligence industry as *EvilCorp*. The group is notorious for its early malware campaigns, such as the Dridex banking trojan. Manatee Tempest is also one of the first groups to be sanctioned by the [Office of Foreign Assets Control \(OFAC\)](#) in 2019. The actor is known for constantly rebranding their malware and shifting tactics to avoid attribution and disassociate themselves from said sanctions.

Manatee Tempest's latest tactics rely on a partnership with Mustard Tempest (DEV-0206), an access broker that facilitates access to target networks. The group has been observed targeting organizations across diverse industries using methods such as drive-by download, including malvertising and [FakeUpdates](#) (also known as SocGholish) infections facilitated by Mustard Tempest to obtain initial access and ultimately deploy ransomware. The actor also uses domain fronting to establish command-and-control channels for Cobalt Strike beacons. As of November 2022, Manatee Tempest continues to leverage [FakeUpdates](#) for initial compromise, followed by the [BLISTER](#) loader to deliver Cobalt Strike Beacons, which are used for lateral movement and ransomware deployment. In July 2023, Microsoft observed Manatee Tempest replacing the Cobalt Strike Beacon payload with a custom Mythic payload.

You can find more information about Manatee Tempest in their Intel Profile.



Looks right

Needs improvement

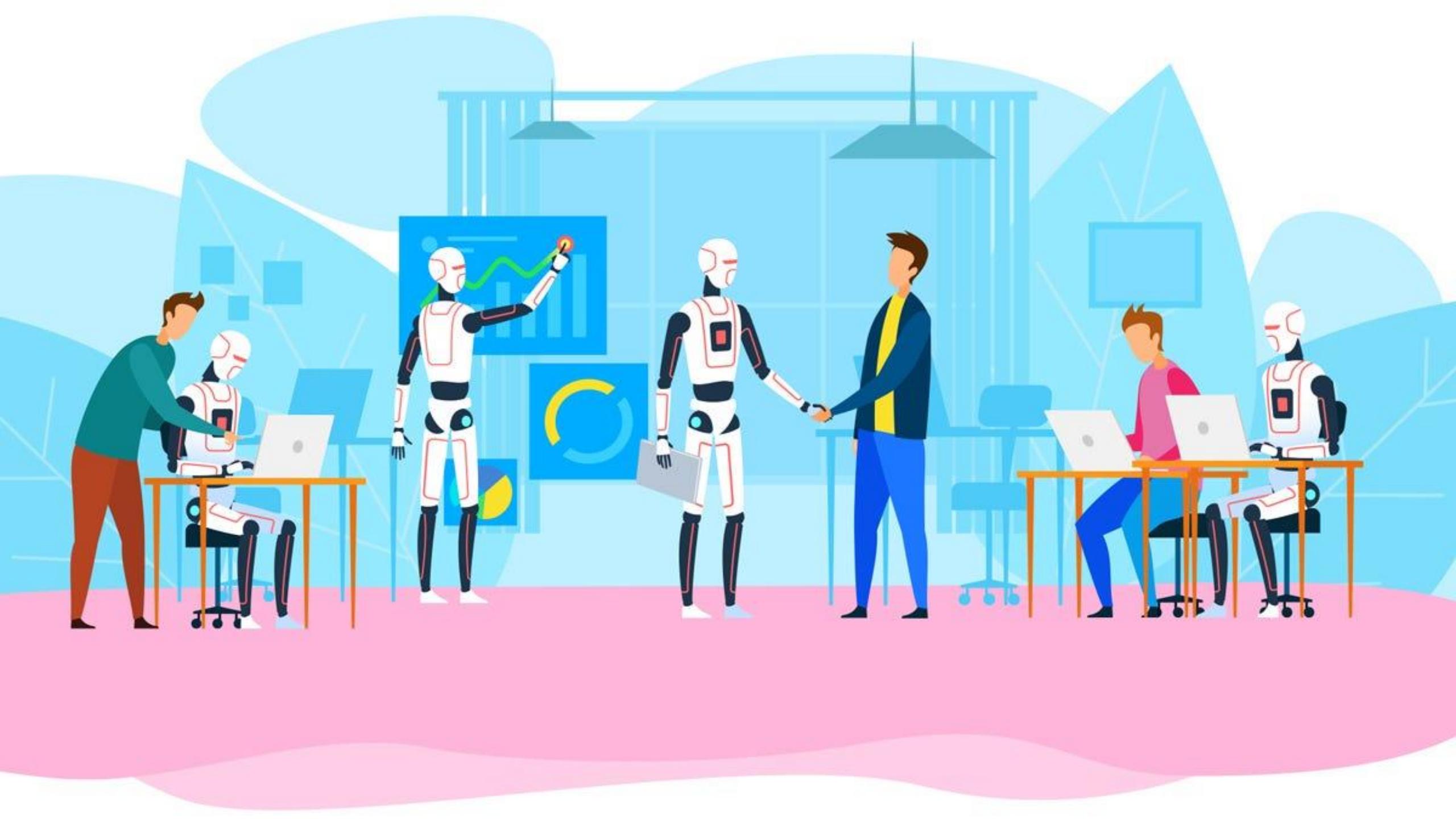
Inappropriate



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









The process of writing, refining, and optimizing inputs - or “**prompts**” – to encourage generative AI systems to create specific, high-quality outputs is called **prompt engineering**.

Explore with Copilot

❖ **Featured Prompts**

📘 Promptbooks

Show high severity Microsoft 365 Defender incidents.

New

Microsoft 365 Defender



Explore with Copilot

❖ **Featured Prompts**

📘 Promptbooks

Suspicious script analysis v3 (Copy)

Get a report analyzing the intent, intelligence, threat actors, and impacts of a suspicious script.

Microsoft Security · 7 prompts



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



Elements of successful prompt

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

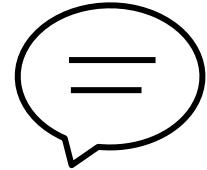
What format or audience do you want the response tailored to?

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

Source

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

"Look in Defender incidents."



What prompts you?



/imagine prompt::a latte skatepark in the middle of the desert in Mars

© John Fowler

Nikon D80

Coyote Buttes, USA

DON'T GIVE UP ON THE REAL WORLD. **Nikon**



Thank you



Darko Todoroski

Cybersecurity Solution Architect



Mirad Maglic

Cybersecurity Sales Executive



